

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平9-330298

(43)公開日 平成9年(1997)12月22日

(51) Int.Cl.⁸ 認別記号 庁内整理番号 F I 技術表示箇所
G 06 F 15/00 3 3 0 G 06 F 15/00 3 3 0 E
1/00 3 7 0 1/00 3 7 0 E

審査請求 未請求 請求項の数12 O L (全 29 頁)

(21)出願番号 特願平8-152578

(22)出願日 平成8年(1996)6月13日

(71)出願人 000006013

三菱電機株式会社

東京都千代田区丸の内二丁目2番3号

(72)発明者 柳原 裕之

東京都千代田区丸

菱電機株式会社内

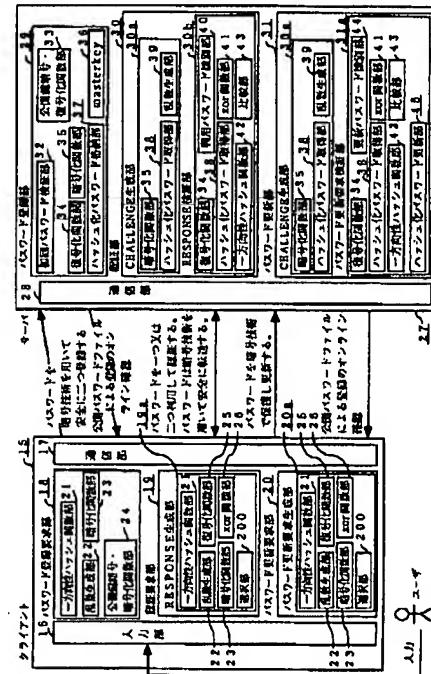
(74)代理人 弁理士 宮田 金雄 (外3名)

(54) 【発明の名称】 パスワード登録方法、認証方法、パスワード更新方法、パスワード登録システム、認証システム
およびパスワード更新システム

(57)【要約】

【課題】 認証に使用するパスワードの個数を利用者側で変更でき、かつ第三者による盗聴に対して安全な認証を行うことが困難であった。

【解決手段】 ユーザはクライアント15の認証要求部19を利用して、パスワードを1つ又は2つ用いてサーバ27に認証してもらう。この時、パスワードは暗号機能を利用して安全にサーバ27に転送される。同時に、クライアント15はサーバ27から受信した複数の乱数の内、認証に用いるパスワードの個数に対応した乱数を選択してサーバ27に対して送信する。サーバ27では認証部30において受信した乱数からパスワードをいくつ用いた認証であるかを確認し、暗号化パスワードを復号化し、得られたパスワードに一方向性関数を適用し、登録してあるハッシュ化パスワードと比較する。一致すれば認証が完了する。



【特許請求の範囲】

【請求項1】 第2処理装置が第1処理装置に対してアクセスする際に用いるパスワードを登録するパスワード登録方法であって、
 上記第2処理装置側の処理として、
 上記第1処理装置に登録すべきパスワードを入力する入力ステップと、
 任意の情報を生成する任意情報生成ステップと、
 上記入力されたパスワード及び上記生成された任意情報を暗号化する第1暗号化ステップと、
 上記暗号化されたパスワード及び暗号化された任意情報を上記第1処理装置に対して送信する送信ステップとを有し、
 上記第1処理装置側の処理として、
 上記暗号化されたパスワード及び上記暗号化された任意情報を受信する受信ステップと、
 上記暗号化されたパスワード及び上記暗号化された任意情報を復号化する復号化ステップと、
 上記復号化されたパスワードを上記復号化された任意情報を用いて暗号化する第2暗号化ステップと、
 上記復号化された任意情報を用いて暗号化されたパスワードを公開する情報公開ステップと、
 上記パスワードを登録する登録ステップとを有することを特徴とするパスワード登録方法。

【請求項2】 複数の登録パスワードが登録された第1処理装置に対して第2処理装置がアクセスすることの妥当性を判断する認証方法であって、
 上記第1処理装置が複数の任意情報を生成し、生成した複数の任意情報を上記第2処理装置に対して送信する第1送信ステップと、
 上記第2処理装置側の処理として、
 上記第1処理装置から送信された複数の任意情報を受信する第1受信ステップと、
 1つ以上の入力パスワードを入力する入力ステップと、
 上記受信した複数の任意情報の中から、上記入力パスワードの数に対応した任意情報を選択する選択ステップと、
 上記選択された任意情報及び上記入力パスワードを上記第1処理装置に対して送信する第2送信ステップとを有し、
 上記第1処理装置側の処理として、
 上記選択された任意情報及び上記入力パスワードを受信する第2受信ステップと、
 上記選択された任意情報に基づき、認証に使用するパスワードの数を認識する認識ステップと、
 上記第1処理装置に登録されている複数の登録パスワードの中から、上記認識結果に対応した数の登録パスワードを取り出す取出ステップと、
 上記取り出された登録パスワードと、上記入力パスワードとの照合を行う照合ステップとを有することを特徴と

する認証方法。

【請求項3】 上記第1受信ステップにおける複数の任意情報は、乱数であることを特徴とする請求項2記載の認証方法。

【請求項4】 上記第2送信ステップは、上記入力された入力パスワードの数にかかわらず、上記入力パスワードを一定の情報量に変換して送信することを特徴とする請求項2または3記載の認証方法。

【請求項5】 複数の登録パスワードが登録された第1処理装置に対して第2処理装置がアクセスすることの妥当性を判断する認証方法であって、
 上記第2処理装置側の処理として、
 第1の入力パスワード及び第2の入力パスワードを入力する入力ステップと、
 上記入力された第1の入力パスワード及び第2の入力パスワードに対し、送信用パスワード及び鍵暗号化用パスワードを対応して指定する指定ステップと、
 上記指定された送信用パスワードを所定情報を用いて暗号化するパスワード暗号化ステップと、
 上記指定された鍵暗号化用パスワードを鍵として、上記所定情報を鍵暗号化する鍵暗号化ステップと、
 上記送信用パスワード及び鍵暗号化用パスワードの指定結果を示す指定情報と、上記暗号化された送信用パスワードと、上記鍵暗号化された所定情報を上記第1処理装置に対して送信する送信ステップとを有し、
 上記第1処理装置側の処理として、
 上記指定情報と、暗号化された送信用パスワードと、鍵暗号化された所定情報を受信する受信ステップと、
 上記指定情報に基づき、上記第1処理装置に登録された複数の登録パスワードの中から上記鍵暗号化用パスワードに対応する第1登録パスワードを選択する選択ステップと、
 上記選択された第1登録パスワードを鍵として、上記鍵暗号化された所定情報を鍵復号化する鍵復号化ステップと、
 上記鍵復号化された所定情報を用い、上記暗号化された送信用パスワードを復号化するパスワード復号化ステップと、
 上記復号化された送信用パスワードと、上記第1処理装置に登録された複数の登録パスワードの内の第2登録パスワードとの照合を行う照合ステップとを有することを特徴とする認証方法。

【請求項6】 上記第2処理装置側の処理として、乱数を生成する乱数発生ステップを有し、
 上記パスワード暗号化ステップは、上記指定された送信用パスワードを上記生成された乱数を用いて暗号化することを特徴とする請求項5記載の認証方法。

【請求項7】 第2処理装置が第1処理装置に対してアクセスする際に用いる登録パスワードを更新するパスワード更新方法であって、

3

上記第1処理装置が複数の任意情報を生成し、生成した複数の任意情報を上記第2処理装置に対して送信する第1送信ステップと、
 上記第2処理装置側の処理として、
 上記第1処理装置から送信された複数の任意情報を受信する第1受信ステップと、
 入力パスワード及び更新パスワードを入力する入力ステップと、
 上記受信した複数の任意情報の中から、上記第1処理装置に登録された複数の登録パスワードの内更新すべき登録パスワードに対応した任意情報を選択する選択ステップと、
 上記入力パスワードと上記更新パスワード及び上記選択された任意情報を上記第1処理装置に対して送信する第2送信ステップと、
 上記第1処理装置側の処理として、
 上記入力パスワードと上記更新パスワード及び上記選択された任意情報を受信する第2受信ステップと、
 上記選択された任意情報により、上記第1処理装置に登録された複数の登録パスワードの中から更新すべき登録パスワードを認識する認識ステップと、
 上記入力パスワードと、上記第1処理装置に登録された複数の登録パスワードの内所定の登録パスワードとの照合を行う照合ステップと、
 上記照合結果に基づき、上記認識結果に対応した登録パスワードを上記更新パスワードに更新する更新ステップとを有することを特徴とするパスワード更新方法。
【請求項8】 上記第1処理装置に登録された登録パスワードの更新は、上記第1処理装置に登録された複数のパスワードの内、任意の登録パスワードについて更新可能であることを特徴とする請求項7記載のパスワード更新方法。

【請求項9】 第2処理装置が第1処理装置に対してアクセスする際に用いるパスワードを登録するパスワード登録システムであって、上記第2処理装置は、
 任意の情報を生成する任意情報生成手段と、
 入力されたパスワード及び上記任意情報生成手段により生成された任意情報を暗号化する第1暗号化手段と、
 上記第1暗号化手段によって暗号化されたパスワード及び任意情報を上記第1処理装置に対して送信する送信手段とを有し、上記第1処理装置は、
 上記暗号化されたパスワード及び上記暗号化された任意情報を受信する受信手段と、
 上記受信手段により受信した上記暗号化されたパスワード及び上記暗号化された任意情報を復号化する復号化手段と、
 上記復号化手段によって復号化されたパスワードを上記復号化手段によって復号化された任意情報を用いて暗号化する第2暗号化手段と、
 上記第2暗号化手段によって暗号化されたパスワードを

4

公開する情報公開手段と、
 上記パスワードを登録する登録手段とを有することを特徴とするパスワード登録システム。
【請求項10】 複数の登録パスワードが登録された第1処理装置に対して第2処理装置がアクセスすることの妥当性を判断する認証システムであって、
 上記第2処理装置は、
 上記第1処理装置から送信された複数の任意情報を受信する第1受信手段と、
 10 上記第1受信手段によって受信した複数の任意情報の中から、入力された入力パスワードの数に対応した任意情報を選択する選択手段と、
 上記選択手段により選択された任意情報及び上記入力された入力パスワードを上記第1処理装置に対して送信する送信手段とを有し、
 上記第1処理装置は、
 上記複数の任意情報を生成する任意情報生成手段と、
 上記選択された任意情報及び上記入力パスワードを上記第2処理装置から受信する第2受信手段と、
 20 上記第2受信手段によって受信した上記選択された任意情報に基づき、認証に使用するパスワードの数を認識する認識手段と、
 上記第1処理装置に登録されている複数の登録パスワードの中から、上記認識結果に対応した数の登録パスワードを取り出す取出手段と、
 上記取出手段によって取り出された登録パスワードと、上記第2受信手段によって受信した入力パスワードとの照合を行う照合手段とを有することを特徴とする認証システム。
 30 【請求項11】 複数の登録パスワードが登録された第1処理装置に対して第2処理装置がアクセスすることの妥当性を判断する認証システムであって、
 上記第2処理装置は、
 入力された第1の入力パスワード及び第2の入力パスワードの内送信用パスワードとして指定された一方の入力パスワードを所定情報を用いて暗号化するパスワード暗号化手段と、
 上記入力された第1の入力パスワード及び第2の入力パスワードの内、鍵暗号化用パスワードとして指定された他方の入力パスワードを鍵として上記所定情報を鍵暗号化する鍵暗号化手段と、
 上記送信用パスワード及び鍵暗号化用パスワードの指定結果を示す指定情報と、上記パスワード暗号化手段によって暗号化された送信用パスワードと、上記鍵暗号化手段によって鍵暗号化された所定情報を上記第1処理装置に対して送信する送信手段とを有し、
 上記第1処理装置は、
 上記送信手段によって送信された上記指定情報と、上記暗号化された送信用パスワードと、上記鍵暗号化された所定情報を受信する受信手段と、
 40 50

5

上記指定情報に基づき、上記第1処理装置に登録された複数の登録パスワードの中から上記鍵暗号化用パスワードに対応する第1登録パスワードを選択する選択手段と、

上記選択手段によって選択された第1登録パスワードを鍵として、上記鍵暗号化された所定情報を鍵復号化する鍵復号化手段と、
上記鍵復号化手段によって鍵復号化された所定情報を用い、上記暗号化された送信用パスワードを復号化するパスワード復号化手段と、

上記パスワード復号化手段によって復号化された送信用パスワードと、上記第1処理装置に登録された複数の登録パスワードの内の第2登録パスワードとの照合を行う照合手段とを有することを特徴とする認証システム。

【請求項12】 第2処理装置が第1処理装置に対してアクセスする際に用いる登録パスワードを更新するパスワード更新システムであって、

上記第2処理装置は、

上記第1処理装置から送信された複数の任意情報を受信する第1受信手段と、
上記第1受信手段により受信した複数の任意情報の中から、上記第1処理装置に登録された複数の登録パスワードの内更新すべき登録パスワードに対応した任意情報を選択する選択手段と、

入力された入力パスワード及び更新パスワードと、上記選択手段によって選択された任意情報を上記第1処理装置に対して送信する送信手段とを有し、

上記第1処理装置は、

上記複数の任意情報を生成する任意情報生成手段と、
上記送信手段によって送信された入力パスワード、更新パスワード及び上記選択された任意情報を受信する第2受信手段と、

上記第2受信手段によって受信した上記選択された任意情報により、上記第1処理装置に登録された複数の登録パスワードの中から更新すべき登録パスワードを認識する認識手段と、

上記第2受信手段によって受信した上記入力パスワードと、上記第1処理装置に登録された複数の登録パスワードの内所定の登録パスワードとの照合を行う照合手段と、

上記照合手段による照合結果に基づき、上記認識手段による認識結果に対応した登録パスワードを上記更新パスワードに更新する更新手段とを有することを特徴とするパスワード更新システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、第1処理装置に対して第2処理装置がアクセスすることの妥当性を判断する認証システムに関するものであり、例えば通信ネットワークで結ばれたクライアント・サーバ間のパスワー

6

ドを用いた認証システムとして用いられるものである。以降、クライアントサーバ間での認証に適用した場合を例に説明する。

【0002】

【從来の技術】從来技術として、Internet Engineering Task Force(IETF)のPoint-to-Point Protocol Working Groupによって提示されている2つの認証プロトコルを以下に示す。1つは、Password Authentication Protocol(以下、PAPと記す)という從来のクライアントサーバ間認証方法で、UNIX™等で採用されている簡単な認証方法である。もうひとつは、Password Handshake Authentication Protocol(以下、CHAPと記す)という從来的一般的なクライアントサーバ間での認証方法である。

【0003】図17は「Brian Lloyd and William Simpson. PPP authentication protocols. RFC 1334, October 1992」に記されるPAPの概要を示す図である。次いで、図18は同じ文献に記されるCHAPの概要を示す図である。

【0004】さらに、図19は、特開平2-162443号公報に記載されている從来の利用者確認方式を示すフローチャートである。この利用者確認方式は、複数のパスワードを用いて利用者の確認を行うものである。

【0005】<從来技術の動作の説明>

【利用する暗号化表記】以降、本明細書では暗号関連の表現に関して以下の表記を使用する。

[data]key ; keyを鍵としてdataを秘密鍵暗号で暗号化する。

Kx+[data] ; 公開鍵Kx+でdataを公開鍵暗号で暗号化する。

Kx-[data] ; 秘密鍵Kx-でdataを公開鍵暗号で復号化する。

h(data) ; dataを一方向性ハッシュ関数にかける。

A@B; AとBの排他的論理和(xor)をとる。

A, B; "AとBの連結"

【0006】[PAPの説明] 図17を用いてPAPの動作原理を説明する。PAPでは、ユーザは安全な手段(オフライン)で、自分のパスワード(passwd)をサーバに登録してもらう。図17における1は認証を要求するクライアントである。ユーザはクライアント1を介してサーバと通信し、認証してもらう。

【0007】2は、ユーザのパスワードを登録・保持するパスワードファイル3と、パスワードファイルから特定のユーザのパスワード情報を検索するパスワードファイル検索部4と、クライアントから受信したパスワードを暗号化する暗号化部5と、暗号化部5の出力とパスワードファイル検索部4の検索結果を比較する比較部6で構成されるサーバである。暗号化部5は公開アルゴリズムを有する。サーバ2は、各ユーザのパスワードを暗号化部5でハッシュ関数h(·)を用いて変換したh(passwd)をユーザのID(以下、IDcと記す)と共にパスワードフ

ファイル③に保管している。

【0008】PAPにおける認証方法を詳述する。図17において、ユーザは、自分のID(IDc)、パスワードpasswdをクライアント1に入力すると、クライアント1は、認証要求(以下、AuthReqと記す)、IDc、パスワードをサーバ2へ送る。サーバ2のパスワードファイル検索部4は、IDcをキーとしてパスワードファイル③を検索し、クライアントの暗号化パスワードh(passwd)を見つける。次に、転送されてきたpasswdを暗号化部5において暗号関数h(・)に適用し、出力結果とパスワードファイル③から得たh(passwd)を比較部6において比較する。この比較の結果、値が同じならばクライアント1(又はユーザ)を正当とみなし、正当に認証した旨“OK”等をクライアントに送信する(値が違えば、認証しなかった旨“NG”等を送信する)。なお、UNIXではパスワードファイルとしてIDcとh(passwd)を他の情報と共に公開しているシステムがある。

【0009】[CHAPの説明] 図18を用いてCHAPの動作原理を説明する。7は、パスワードを変換する一方向性ハッシュ関数部8で構成されるクライアントである。9は、乱数を生成する乱数生成部10と、ユーザのパスワードを登録・保持するパスワードファイル11と、パスワードファイル11から特定のユーザとパスワード情報を検索するパスワードファイル検索部12と、クライアントから受信したパスワードを変換する一方向性ハッシュ関数部13と、一方向性ハッシュ関数部13の出力とクライアント7から受信したデータを比較する比較部14で構成されるサーバである。一方向性ハッシュ関数部8、13は同一の公開アルゴリズムを有する。サーバ9は、各クライアントのIDとそのパスワードを秘密にパスワードファイル11に保管している。ユーザはクライアント7を介してサーバ9に認証してもらう。

【0010】CHAPにおける認証方法を説明する。クライアント7とサーバ9でコネクションがはられると、サーバ9の乱数生成部10は、challengeという乱数を生成し、クライアント7に送る。クライアント7はこれを受信すると、ユーザはIDであるIDcと、パスワードpasswdをクライアント7に入力する。クライアント7はIDc、passwd、challengeを一方向性ハッシュ関数部8に入力し、出力h(IDc, passwd, challenge)をIDcと共にサーバへ送信する。

【0011】サーバ9は、受信したIDcをキーとしてパスワードファイル検索部12を利用してパスワードファイル11を検索し、ユーザのpasswdを見つける。次にIDc、passwd、challengeを一方向性ハッシュ関数部13に入力し、出力結果h(IDc, passwd, challenge)と受信した値を比較部14において比較する。値が一致していればクライアント7(又はユーザ)はpasswdを知っているとみなし、正当に認証した旨“OK等”をクライアント7に送信する(値が違えば、認証しなかった旨“N

G”等を送信する)。

【0012】[特開平2-162443号公報の説明] 図19を用いて特開平2-162443号公報に示された利用者確認方法を説明する。この利用者確認方法では、あらかじめ複数個のパスワードをセンタに登録しておき、ユーザから一定時間以内にパスワードの入力があると、入力されたパスワードPWと登録されている複数個のパスワードPW1～PWaとの照合を行う(ステップ206)。

10 【0013】照合の結果、PWがPW1～PWaのいずれかと一致すれば、カウンタC1を1インクリメントする(ステップ208)。インクリメントの結果、カウンタC1の値が一致すべきパスワード数Sに達した場合には、ユーザのアクセスを許可する(ステップ210)。 【0014】照合の結果、PWがPW1～PWaのいずれかと一致しなければ、カウンタC2を1インクリメントする(ステップ211)。インクリメントの結果、カウンタC2の値が一定数以上となった場合には、ユーザのアクセスを不許可としてパスワード照合を終了する(ステップ213)。

【0015】 【発明が解決しようとする課題】 PAP方式に関しては、図17に示すようにユーザのパスワードpasswdは保護されずネットワーク上を転送されるので、第三者にパスワードを盗聴されると、この第三者が正当なユーザになりますことができる。又、パスワードファイル③が公開されているシステムでは、ファイルにIDcとh(passwd)の組み合わせがあるので、攻撃者はパスワードファイル上の任意のIDcとh(passwd)に対してオフラインで辞書攻撃を行うことができる。

【0016】又、クライアント1はサーバ2が正当なサーバであるかどうかを確認することができない。さらに、パスワードを更新したとしても、更新パスワード(新しいパスワード)をサーバに転送するときに第三者が盗聴すれば、盗聴した更新パスワードを利用できてしまい危険である、等の問題があった。

【0017】一方CHAP方式に関しては、図18に示すように、盗聴者はIDc、challenge、h(IDc, passwd, challenge)を盗聴できるので、考えるユーザのパスワードpasswd■をIDc、challengeとともにh()に入力し、h(IDc, passwd, challenge)と一致するまでpasswd■をえて、passwdを割り出すことが可能である。

【0018】又、パスワードが一つしか利用できないので、この様な方法で割り出された場合はユーザの安全性が危うくなる。さらに、サーバ9は、IDcとpasswdを秘密に保持しなくてはならないので、クライアントが登録状況の確認を行うこと及び、安全性を確保する上で重要なパスワードの変更もサーバとオフラインで行わなくてはならず不便である、等の問題があった。

50 【0019】さらに、特開平2-162443号公報に

示された利用者確認方法に関しては、複数のパスワードを利用しているが、複数のパスワードを入力するのみで、暗号技術によるパスワードの保護は行っていないため、ユーザが入力したパスワードをセンタに送信する際に盗聴される恐れがあり危険であるという問題があった。また、ユーザは、登録した複数のパスワードを選択的に用いることはできず、常に一定数以上のパスワードを入力する必要があった。

【0020】この発明は上記のような問題点を解消するためになされたもので、以下のような特徴を持った方式を得ることを目的とする。第1の目的は、パスワードの登録に際し、パスワードが正常に登録されたか否かを利用者が確認できるとともに、第3者によって登録したパスワードが解読されることを防止するパスワード登録方法及び装置を得ることである。

【0021】第2の目的は、登録した複数のパスワードの内いずれのパスワードを用いても認証でき、かつ第3者によっていくつのパスワードを用いて認証を行っているのかを解読されるのを防止する認証方法及び装置を得ることを目的とする。

【0022】第3の目的は、複数のパスワードを用いて第3者による解読をより困難にするとともに、送信する情報量を削減することができる認証方法および装置を得ることを目的とする。

【0023】

【課題を解決するための手段】第1の発明におけるパスワード登録方法は、第2処理装置が第1処理装置に対してアクセスする際に用いるパスワードを登録するパスワード登録方法であって、上記第2処理装置側の処理として、上記第1処理装置に登録すべきパスワードを入力する入力ステップと、任意の情報を生成する任意情報生成ステップと、上記入力されたパスワード及び上記生成された任意情報を暗号化する第1暗号化ステップと、上記暗号化されたパスワード及び暗号化された任意情報を上記第1処理装置に対して送信する送信ステップとを有し、上記第1処理装置側の処理として、上記暗号化されたパスワード及び上記暗号化された任意情報を受信する受信ステップと、上記暗号化されたパスワード及び上記暗号化された任意情報を復号化する復号化ステップと、上記復号化されたパスワードを上記復号化された任意情報を用いて暗号化する第2暗号化ステップと、上記復号化された任意情報を用いて暗号化されたパスワードを公開する情報公開ステップと、上記パスワードを登録する登録ステップとを有するものである。ここで、入力ステップは後述の実施の形態におけるS1に対応し、任意情報生成ステップはS2に対応し、第1暗号化ステップはS301及びS302に対応し、送信ステップはS4に対応する。また、受信ステップはS5に対応し、復号化ステップはS61及びS62に対応し、第2暗号化ステップはS7に対応し、情報公開ステップはS8に対応

し、登録ステップはS9に対応する。

【0024】第2の発明における認証方法は、複数の登録パスワードが登録された第1処理装置に対して第2処理装置がアクセスすることの妥当性を判断する認証方法であって、上記第1処理装置が複数の任意情報を生成し、生成した複数の任意情報を上記第2処理装置に対して送信する第1送信ステップと、上記第2処理装置側の処理として、上記第1処理装置から送信された複数の任意情報を受信する第1受信ステップと、1つ以上の入力

10 パスワードを入力する入力ステップと、上記受信した複数の任意情報の中から、上記入力パスワードの数に対応した任意情報を選択する選択ステップと、上記選択された任意情報及び上記入力パスワードを上記第1処理装置に対して送信する第2送信ステップとを有し、上記第1処理装置側の処理として、上記選択された任意情報及び上記入力パスワードを受信する第2受信ステップと、上記選択された任意情報に基づき、認証に使用するパスワードの数を認識する認識ステップと、上記第1処理装置に登録されている複数の登録パスワードの中から、上記認識結果に対応した数の登録パスワードを取り出す取出ステップと、上記取り出された登録パスワードと、上記入力パスワードとの照合を行う照合ステップとを有するものである。ここで、第1送信ステップは後述の実施の形態におけるS11及びS12に対応し、第1受信ステップはS13に対応し、入力ステップはS14に対応し、選択ステップはS16に対応し、第2送信ステップはS19に対応する。第2受信ステップはS20に対応し、認識ステップはS21に対応し、取出ステップはS22に対応し、照合ステップはS25に対応する。

20 【0025】第3の発明における認証方法は、上記第2の発明において上記第1受信ステップにおける複数の任意情報が、乱数であることを特徴とするものである。

【0026】第4の発明における認証方法は、上記第2または第3の発明において、上記第2送信ステップが、上記入力された入力パスワードの数にかかわらず、上記入力パスワードを一定の情報量に変換して送信するものである。

【0027】第5の発明における認証方法は、複数の登録パスワードが登録された第1処理装置に対して第2処理装置がアクセスすることの妥当性を判断する認証方法であって、上記第2処理装置側の処理として、第1の入力パスワード及び第2の入力パスワードを入力する入力ステップと、上記入力された第1の入力パスワード及び第2の入力パスワードに対し、送信用パスワード及び鍵暗号化用パスワードを対応して指定する指定ステップと、上記指定された送信用パスワードを所定情報を用いて暗号化するパスワード暗号化ステップと、上記指定された鍵暗号化用パスワードを鍵として、上記所定情報を鍵暗号化する鍵暗号化ステップと、上記送信用パスワード及び鍵暗号化用パスワードの指定結果を示す指定情報

50 50

11

と、上記暗号化された送信用パスワードと、上記鍵暗号化された所定情報を上記第1処理装置に対して送信する送信ステップとを有し、上記第1処理装置側の処理として、上記指定情報と、暗号化された送信用パスワードと、鍵暗号化された所定情報を受信する受信ステップと、上記指定情報に基づき、上記第1処理装置に登録された複数の登録パスワードの中から上記鍵暗号化用パスワードに対応する第1登録パスワードを選択する選択ステップと、上記選択された第1登録パスワードを鍵として、上記鍵暗号化された所定情報を鍵復号化する鍵復号化ステップと、上記鍵復号化された所定情報を用い、上記暗号化された送信用パスワードを復号化するパスワード復号化ステップと、上記復号化された送信用パスワードと、上記第1処理装置に登録された複数の登録パスワード内の第2登録パスワードとの照合を行う照合ステップとを有するものである。ここで、入力ステップは後述の実施の形態におけるS14に対応し、指定ステップはS15に対応し、パスワード暗号化ステップはS18に対応し、鍵暗号化ステップはS17に対応し、送信ステップはS19に対応する。受信ステップはS20に対応し、選択ステップはS20に対応し、鍵復号化ステップはS23に対応し、パスワード復号化ステップはS24に対応し、照合ステップはS25に対応する。

【0028】第6の発明における認証方法は、第5の発明にさらに上記第2処理装置側の処理として、乱数を生成する乱数発生ステップを有し、上記パスワード暗号化ステップが、上記指定された送信用パスワードを上記生成された乱数を用いて暗号化するものである。

【0029】第7の発明におけるパスワード更新方法は、第2処理装置が第1処理装置に対してアクセスする際に用いる登録パスワードを更新するパスワード更新方法であって、上記第1処理装置が複数の任意情報を生成し、生成した複数の任意情報を上記第2処理装置に対して送信する第1送信ステップと、上記第2処理装置側の処理として、上記第1処理装置から送信された複数の任意情報を受信する第1受信ステップと、入力パスワード及び更新パスワードを入力する入力ステップと、上記受信した複数の任意情報の中から、上記第1処理装置に登録された複数の登録パスワードの内更新すべき登録パスワードに対応した任意情報を選択する選択ステップと、上記入力パスワードと上記更新パスワード及び上記選択された任意情報を上記第1処理装置に対して送信する第2送信ステップと、上記第1処理装置側の処理として、上記入力パスワードと上記更新パスワード及び上記選択された任意情報を受信する第2受信ステップと、上記選択された任意情報により、上記第1処理装置に登録された複数の登録パスワードの中から更新すべき登録パスワードを認識する認識ステップと、上記入力パスワードと、上記第1処理装置に登録された複数の登録パスワードの内所定の登録パスワードとの照合を行う照合ステッ

12

プと、上記照合結果に基づき、上記認識結果に対応した登録パスワードを上記更新パスワードに更新する更新ステップとを有するものである。ここで、第1送信ステップは後述の実施の形態におけるS31及びS32に対応し、第1受信ステップはS33に対応し、入力ステップはS34に対応し、選択ステップはS35に対応し、第2送信ステップはS36に対応する。第2受信ステップはS37に対応し、認識ステップはS38に対応し、照合ステップはS39に対応し、更新ステップはS301に対応する。

【0030】第8の発明は、第7の発明においてさらに上記第1処理装置に登録された登録パスワードの更新が、上記第1処理装置に登録された複数のパスワードの内、任意の登録パスワードについて更新可能としたものである。

【0031】第9の発明におけるパスワード登録システムは、第2処理装置が第1処理装置に対してアクセスする際に用いるパスワードを登録するパスワード登録システムであって、上記第2処理装置が、任意の情報を生成する任意情報生成手段と、入力されたパスワード及び上記任意情報生成手段により生成された任意情報を暗号化する第1暗号化手段と、上記第1暗号化手段によって暗号化されたパスワード及び任意情報を上記第1処理装置に対して送信する送信手段とを有し、上記第1処理装置が、上記暗号化されたパスワード及び上記暗号化された任意情報を受信する受信手段と、上記受信手段により受信した上記暗号化されたパスワード及び上記暗号化された任意情報を復号化する復号化手段と、上記復号化手段によって復号化されたパスワードを上記復号化手段によって復号化された任意情報を用いて暗号化する第2暗号化手段と、上記第2暗号化手段によって暗号化されたパスワードを公開する情報公開手段と、上記パスワードを登録する登録手段とを有するものである。ここで、第1暗号化手段は後述の実施の形態における一方向性ハッシュ関数部21、暗号化関数部23、公開鍵暗号・暗号化関数部24に対応し、復号化手段は復号化関数部34及び公開鍵暗号・暗号化関数部33に対応し、第2暗号化手段は暗号化関数部35に対応し、情報公開手段は公開パスワードファイル37aに対応し、登録手段は非公開パスワードファイル37bに対応する。

【0032】第10の発明における認証システムは、複数の登録パスワードが登録された第1処理装置に対して第2処理装置がアクセスすることの妥当性を判断する認証システムであって、上記第2処理装置が、上記第1処理装置から送信された複数の任意情報を受信する第1受信手段と、上記第1受信手段によって受信した複数の任意情報の中から、入力された入力パスワードの数に対応した任意情報を選択する選択手段と、上記選択手段により選択された任意情報及び上記入力された入力パスワードを上記第1処理装置に対して送信する送信手段とを有

13

し、上記第1処理装置が、上記複数の任意情報を生成する任意情報生成手段と、上記選択された任意情報及び上記入力パスワードを上記第2処理装置から受信する第2受信手段と、上記第2受信手段によって受信した上記選択された任意情報に基づき、認証に使用するパスワードの数を認識する認識手段と、上記第1処理装置に登録されている複数の登録パスワードの中から、上記認識結果に対応した数の登録パスワードを取り出す取出手段と、上記取出手段によって取り出された登録パスワードと、上記第2受信手段によって受信した入力パスワードとの照合を行う照合手段とを有するものである。ここで、選択手段は後述の実施の形態における選択部200に対応し、任意情報生成手段は乱数生成部22に対応し、認識手段は利用パスワード識別部40に対応し、取出手段はハッシュ化パスワード取得部38に対応し、照合手段は比較部43に対応する。

【0033】第11における認証システムは、複数の登録パスワードが登録された第1処理装置に対して第2処理装置がアクセスすることの妥当性を判断する認証システムであって、上記第2処理装置が、入力された第1の入力パスワード及び第2の入力パスワードの内送信用パスワードとして指定された一方の入力パスワードを所定情報を用いて暗号化するパスワード暗号化手段と、上記入力された第1の入力パスワード及び第2の入力パスワードの内、鍵暗号化用パスワードとして指定された他方の入力パスワードを鍵として上記所定情報を鍵暗号化する鍵暗号化手段と、上記送信用パスワード及び鍵暗号化用パスワードの指定結果を示す指定情報と、上記パスワード暗号化手段によって暗号化された送信用パスワードと、上記鍵暗号化手段によって鍵暗号化された所定情報を上記第1処理装置に対して送信する送信手段とを有し、上記第1処理装置が、上記送信手段によって送信された上記指定情報と、上記暗号化された送信用パスワードと、上記鍵暗号化された所定情報を受信する受信手段と、上記指定情報に基づき、上記第1処理装置に登録された複数の登録パスワードの中から上記鍵暗号化用パスワードに対応する第1登録パスワードを選択する選択手段と、上記選択手段によって選択された第1登録パスワードを鍵として、上記鍵暗号化された所定情報を鍵復号化する鍵復号化手段と、上記鍵復号化手段によって鍵復号化された所定情報を用い、上記暗号化された送信用パスワードを復号化するパスワード復号化手段と、上記パスワード復号化手段によって復号化された送信用パスワードと、上記第1処理装置に登録された複数の登録パスワードの内の第2登録パスワードとの照合を行う照合手段とを有するものである。ここで、パスワード暗号化手段は後述の実施の形態におけるxor関数部26に対応し、鍵暗号化手段は暗号化関数部23に対応し、鍵復号化手段は復号化関数部34に対応し、パスワード復号化手段はxor関数部41に対応し、照合手段は比較部43

14

に対応する。

【0034】第12の発明におけるパスワード更新システムは、第2処理装置が第1処理装置に対してアクセスする際に用いる登録パスワードを更新するパスワード更新システムであって、上記第2処理装置が、上記第1処理装置から送信された複数の任意情報を受信する第1受信手段と、上記第1受信手段により受信した複数の任意情報の中から、上記第1処理装置に登録された複数の登録パスワードの内更新すべき登録パスワードに対応した

- 10 任意情報を選択する選択手段と、入力された入力パスワード及び更新パスワードと、上記選択手段によって選択された任意情報を上記第1処理装置に対して送信する送信手段とを有し、上記第1処理装置が、上記複数の任意情報を生成する任意情報生成手段と、上記送信手段によって送信された入力パスワード、更新パスワード及び上記選択された任意情報を受信する第2受信手段と、上記第2受信手段によって受信した上記選択された任意情報により、上記第1処理装置に登録された複数の登録パスワードの中から更新すべき登録パスワードを認識する認識手段と、上記第2受信手段によって受信した上記入力パスワードと、上記第1処理装置に登録された複数の登録パスワードの内所定の登録パスワードとの照合を行う照合手段と、上記照合手段による照合結果に基づき、上記認識手段による認識結果に対応した登録パスワードを上記更新パスワードに更新する更新手段とを有するものである。ここで、任意情報生成手段とは後述の実施の形態における乱数生成部39に対応し、認識手段は更新パスワード識別部44に対応し、照合手段は比較部43に対応し、更新手段はハッシュ化パスワード更新部4.5に対応する。

【0035】

【発明の実施の形態】

実施の形態1. この実施の形態におけるクライアント・サーバ間の認証システムは、2つのパスワードを登録し、登録した2つのパスワードを選択的に用いて認証することができるものであり、以下図1～12を用いて説明する。この実施の形態において利用する暗号化に関する表記は、上述の〔従来の技術の動作の説明〕における表記と同じである。この実施の形態において用いる秘匿化の方式としては、「Bruce Schneier, ■APPLIED CRYPTOGRAPHY second edition■, John Wiley & Sons, Inc, 1995」に記載されている次のような方式が該当する：公開鍵暗号化の方式としては、例えばRSA、Elgamal等がある。また、秘密鍵暗号化の方式としては、例えばDES(Data Encryption Standard)、IDEA(International Data Encryption Algorithm)等がある。

一方向性ハッシュ関数としては、例えばMD4(Message Digest 4)、MD5(MessageDigest 5)、SHA(Secure Hash Algorithm)等がある。一方向性とは、関数 $h(\cdot)$ と変数 a とが与えられると、 $h(a)$ は容易

50

15

に計算できるが、 $h(a)$ の逆関数を求める効率の良い計算法がないことをいう。

【0036】まず、図1を用いてこの実施の形態の概要を説明する。図1において、15は、パスワード及びパラメータを入力する入力部16と、データをネットワークを介して送受信する通信部17と、パスワードの登録要求をサーバに対して行うパスワード登録要求部18と、認証の要求をサーバに対して行う認証要求部19と、パスワードの更新要求をサーバへ行うパスワード更新要求部20とからなるクライアントである。

【0037】パスワード登録要求部18は、入力された情報を一方向性ハッシュ関数にかける一方向性ハッシュ関数部21と、乱数を出力する乱数生成部22と、秘密鍵暗号アルゴリズムを有する暗号化関数部23と、公開鍵暗号アルゴリズムを有する公開鍵暗号・暗号化関数部24とから構成される。

【0038】また、認証要求部19は、入力された情報を一方向性ハッシュ関数にかける一方向性ハッシュ関数部21と、乱数を出力する乱数生成部22と、秘密鍵暗号アルゴリズムを有する暗号化関数部23と、秘密鍵暗号アルゴリズムを有する復号化関数部25と、排他的論理和を計算するxor関数部26と、サーバから受信した情報の中から必要な情報を選択する選択部200とから構成されるRESPONSE生成部19aを有する。

【0039】パスワード更新要求部20は、入力された情報を一方向性ハッシュ関数にかける一方向性ハッシュ関数部21と、乱数を出力する乱数生成部22と、秘密鍵暗号アルゴリズムを有する暗号化関数部23と、公開鍵暗号アルゴリズムを有する復号化関数部25と、xor関数部26と、サーバから受信した情報の中から必要な情報を選択する選択部200とから構成されるパスワード更新要求生成部20aを有する。27は、データをネットワークを介して送受信する通信部28と、パスワードの登録を行うパスワード登録部29と、クライアント15(若しくはユーザ)を認証する認証部30と、パスワードの更新を行うパスワード更新部31とから構成されるサーバである。

【0040】パスワード登録部29は、秘密鍵暗号アルゴリズムを有する暗号化関数部35と、秘密鍵暗号アルゴリズムを有する復号化関数部34と、公開鍵暗号アルゴリズムを有する公開鍵暗号・復号化関数部33と、サーバ27がユーザを一番最初に認証するために機能する初回パスワード検証部32と、パスワード情報を登録・保存するハッシュ化パスワード格納部37とから構成される。

【0041】認証部30は、後述のCHALLENGE生成部30aと、RESPONSE検証部30bとから構成される。CHALLENGE生成部30aは、ハッシュ化されたパスワードを取り出すハッシュ化パスワード取得部38と、乱数生成部39と、秘密鍵暗号アルゴリズムを有する暗号化関数部

16

35からなる。

【0042】RESPONSE検証部30bは、秘密鍵暗号アルゴリズムを有する復号化関数部34と、排他的論理和を計算するxor関数部41と、一方向性ハッシュ関数部42と、クライアント15から転送されてきたユーザのパスワード情報とサーバ27が保持しているパスワード情報を比較する比較部43と、転送されてきたパスワードを識別する利用パスワード識別部40と、ハッシュ化パスワード取得部38からなる。

10 【0043】パスワード更新部31は、CHALLENGE生成部30aと、パスワード更新要求検証部31aとから構成される。パスワード更新部31に設けられるCHALLENGE生成部30aは、認証部30に設けられるCHALLENGE生成部30aと同様の構成であるので説明は省略する。

【0044】パスワード更新要求検証部31aは、秘密鍵暗号アルゴリズムを有する復号化関数部34と、一方向性ハッシュ関数部42と、xor関数部41と、比較部43と、更新するパスワードを区別する更新パスワード識別部44と、ハッシュ化パスワード更新部45と、ハッシュ化パスワード取得部38から構成されるパスワード更新要求検証部31aで構成される。

【0045】尚、公開鍵暗号アルゴリズムを有する公開鍵暗号・暗号化関数部24と、公開鍵暗号・復号化関数部33には、“公開鍵暗号”という名前がついているのに対し、秘密鍵暗号アルゴリズムを有する暗号関数部23、35、秘密鍵暗号アルゴリズムを有する復号関数部25、34に関しては、“秘密鍵暗号”という名前はついていない。前者に対して後者は実施の形態において頻繁に使用するので、煩雑性をさけるため、“秘密鍵暗号”という名前を省略している。

【0046】実施の形態1では、パスワードを二つ利用したクライアント・サーバ間認証システムにおいて、パスワードの登録、パスワードを二つ用いた認証、パスワードの更新について説明する。

【0047】[パスワードの登録]実施の形態1のクライアント・サーバ間認証システムにおいて、ユーザのパスワードをサーバ27へ登録する方法について図1～図3を用いて説明する。ユーザのパスワードの登録は、図1におけるクライアント15のパスワード登録要求部18とサーバ27のパスワード登録部29で動作する。図2は、図1におけるパスワード登録に関する部分を抜粋したものである。

【0048】図2において、18は、パスワードを変換する一方向性ハッシュ関数部21と、乱数を出力する乱数生成部22と、秘密鍵暗号アルゴリズムを有する暗号化関数部23と、公開鍵暗号アルゴリズムを有する公開鍵暗号・暗号化関数部24からなるパスワード登録要求部である。

【0049】29は、パスワード登録時に最初に認証を行う初回パスワード検証部32と、秘密鍵暗号アルゴリ

50

17

ズムを有する復号化関数部34と、公開鍵暗号アルゴリズム有する公開鍵暗号・復号化関数部33と、秘密鍵暗号アルゴリズムを有する暗号化関数部35と、パスワードを登録するハッシュ化パスワード格納部37から構成される、パスワード登録部である。

【0050】次に、ユーザのパスワードをサーバ27へ登録する場合の動作について説明する。サーバ27は、一番最初にユーザを登録するとき（例えば、アカウントの生成の際等）に、パスワードpasswd0を一つ生成してユーザに秘密に渡す。このパスワードpasswd0は、ユーザに対してオフラインで渡される。このパスワードpasswd0は、ユーザが自分で生成したパスワードを登録するときに、サーバに認証してもらうために利用するもので、初回パスワードと呼び、ユーザを登録する際に一度限りしか利用されない。サーバ27は、初回パスワード検証部32においてユーザのIDと初回パスワードの対を保持している。

【0051】ユーザは、図2のクライアントの入力部16に、登録したいパスワードpasswd1,passwd2、自分のID(以下、IDcと記す)、初回パスワードpasswd0、登録要求RegReqを入力する（S1）。入力したこれらのデータは、パスワード登録要求部18に渡される。

【0052】また、乱数生成部22は、3つの乱数rand1、rand2、Rkeyを生成する（S2）。

【0053】パスワード登録要求部18において、一方向性ハッシュ関数部21はpasswd1を入力とし、 $h(passwd1)$ を出力する。この出力と乱数生成部22で生成した乱数rand1が連結され $h(passwd1), rand1$ となる。次に、連結した結果を暗号化関数部23は、乱数生成部22で生成した暗号鍵Rkeyを用いて $h(passwd1), rand1$ を暗号化し、 $[h(passwd1), rand1]Rkey$ を出力する。

【0054】次に、一方向性ハッシュ関数部21はpasswd2を入力として $h(passwd2)$ を出力する。この出力は、乱数生成部22で生成した乱数rand2と連結され、 $h(passwd2), rand2$ となる。この一方向性ハッシュ関数部21および暗号化関数部23の処理をS301とする。

【0055】次いで、公開鍵暗号・暗号化関数部24はRkeyをサーバの公開鍵Ks+を用いて暗号化し、Ks+[Rkey]を出力する（S302）。公開鍵Ks+は、秘密鍵Ks-に対応した情報であるが、公開鍵Ks+のみがクライアントに対して公開され、秘密鍵Ks-はサーバのみが有している。以上の結果と、IDc, RegReq(登録要求), passwd0を連結して、サーバ27へ転送する（S4）。図2においては、連結部を○で示している。

【0056】すなわちRegReq, IDc, passwd0, $[h(passwd1), rand1]Rkey, [h(passwd2), rand2]Rkey, Ks+[Rkey]$ を転送する。転送するユーザのパスワード情報 $h(passwd1), h(passwd2)$ は各々クライアント内で発生した乱数rand1, rand2と連結され、 $h(passwd1), rand1, h(pa$

18

sswd2), rand2

となり、これらはRkeyで暗号化されるので、盗聴からは保護される。

【0057】又、乱数Rkeyもサーバの公開鍵Ks+で暗号化されるので、乱数Rkeyは、サーバ以外には漏洩することはない。したがって、乱数Rkeyが解読されることにより、 $[h(passwd1), rand1]Rkey$ 等が順次解読されることを防止することができる。

【0058】サーバ27では、通信部28を介して、受信データがパスワード登録部29に渡される（S5）。

10 次いで、パスワード登録部29では、IDcとpasswd0の対が正しい組み合わせかを初回パスワード検証部32で検査する。

【0059】IDcとpasswd0の組み合わせが正しくなければ、拒否の通知をクライアント15へ転送する。従って、第三者はIDcで示されるユーザに成りますことはできない。さらに、passwd0はIDcで示されるユーザが、自分で生成した二つのパスワードを初めて登録する場合のみに使用され、それ以降は利用されないので、passwd0を盗聴した第三者がpasswd0を用いて、次回このユーザに成りますとしても成功しない。

【0060】IDcとpasswd0の組み合わせが正しければ、公開鍵暗号・復号化関数部33で、サーバ27の公開鍵暗号の秘密鍵Ks-を用いて受信データのKs+[Rkey]を復号化し、Rkeyを出力する（S62）。かかる秘密鍵Ks-は、サーバ27だけが認識している情報である。

【0061】復号化関数部34は、Rkeyを用いて $[h(passwd1), rand1]Rkey$ を復号化し、 $h(passwd1), rand1$ を出力する。次に、暗号化関数部35は、 $h(passwd1)$ をRkeyで暗号化し、 $[h(passwd1)]Rkey$ を出力する。次いで、復号化関数部34は、Rkeyを用いて $[h(passwd2), rand2]Rkey$ を復号化し、 $h(passwd2), rand2$ を出力する。次に、暗号化関数部35は、 $h(passwd2)$ をRkeyで暗号化し、 $[h(passwd2)]Rkey$ を出力する。この復号化関数部34の処理をS61とし、暗号化関数部35の処理をS7とする。

【0062】次いで、暗号化関数部35はサーバ27のみが秘密に保持するmasterkey36を用いてRkeyを暗号化する。かかるmasterkey36としては、クライアント若しくはユーザごとに異なる情報を設定することも可能であり、その方が安全性が高くなるが、この実施の形態においては、masterkey36として同一の情報を設定するものとして説明する。

【0063】次いで、ハッシュ化パスワード格納部37において、図3に示すように公開鍵パスワードファイル37aと非公開パスワードファイル37bにパスワードに関する情報を格納する。

【0064】すなわち、公開パスワードファイル37aには、一行に $rand1, [h(passwd1)]Rkey, rand2, [h(passwd1)]Rkey$ を登録する。非公開パスワードファイル37bには、IDc, rand1, $[h(passwd1)]Rkey, rand2, [h(pa$

19

swd1)Rkey,[Rkey]masterkeyを登録する。

【0065】次に、サーバ27は、公開パスワードファイル37aをユーザに公開する(S8)。公開は、サーバ27からクライアント15に対して公開パスワードファイル37aの情報を送信することによって公開してもよく、また、クライアント15がサーバ27内の公開パスワードファイル37aにアクセスできるようにして実現してもよい。ユーザはクライアント15の暗号化関数部23を利用して[h(passwd1)]Rkey,[h(passwd2)]Rkeyを計算しておく。

【0066】クライアント15は、公開パスワードファイル37aの情報を受信し、rand1が先頭に登録されている行を検索し、公開パスワードファイル37aにrand1,[h(passwd1)]Rkey,rand2,[h(passwd1)]Rkeyがあることを確かめる。この時、登録の確認は、公開ファイルである公開パスワードファイル37aをオンラインで確認することにより実現可能なので、ユーザにとっては便利である。

【0067】ここで、公開パスワードファイル37aには、クライアント15を利用しているユーザを識別する情報IDcは格納されないため、第三者に公開されることなく、rand1,[h(passwd1)]Rkey,rand2,[h(passwd1)]Rkeyの値を知っているユーザのみが自分のパスワードが登録されていることを知る。

【0068】ユーザを識別する情報IDcは公開されないため、第三者は公開されている公開パスワードファイル37aを見ても、どの情報が誰のものであるか解らないので、ユーザのパスワード解析に役立てられない。又、ハッシュ化パスワードもRkeyで暗号化されているので第三者はハッシュ化パスワード自体をることはできない。

【0069】非公開パスワードファイル37bは、サーバ27のみが秘密に保持するものであり、IDcと暗号化された登録情報(ハッシュ化パスワード)を登録する(S9)。万が一、このファイルの内容が漏洩したとしても、ハッシュ化されたパスワードはRkeyで暗号化されて保護されるのでユーザの安全性は保たれる。

【0070】この実施の形態で述べているハッシュ化や鍵暗号化は、広義の暗号化であるといえる。したがって、一方向性ハッシュ関数部21および暗号化関数部23によって行われる処理S301は、passwd1,passwd2を暗号化するための処理と考えることができる。また、この実施の形態では、passwd1,passwd2の暗号化の処理S301と、Rkeyの暗号化の処理S302を全て実行してからRegReq, IDc, passwd0,[h(passwd1),rand1]Rkey,[h(passwd2),rand2]Rkey,Ks+[Rkey]からなる情報をサーバに対して送信する処理S4を行っている。しかし、処理S301を行ってから[h(passwd1),rand1]Rkey,[h(passwd2),rand2]Rkeyをサーバに対して送信する処理を行い、その後処理S302を行ってか

20

らKs+[Rkey]をサーバに対して送信する処理を行うこともできる。このような場合であっても、入力されたパスワードhを暗号化及び生成された乱数を暗号化するステップと、暗号化されたパスワード及び暗号化された乱数を受信するステップとを備えていることになる。

【0071】また、この実施の形態においてはRegReq, IDc, passwd0,[h(passwd1),rand1]Rkey,[h(passwd2),rand2]Rkey,Ks+[Rkey]からなる情報をすべて受信してから(S5)、[h(passwd1),rand1]Rkey,[h(passwd2),rand2]Rkey及びKs+[Rkey]の復号化のための処理S61, S62を行っているが、上記すべての情報を一括して受信する必要はなく、まずRegReq, IDc, passwd0,Ks+[Rkey]を受信してKs+[Rkey]の復号化(S62)を行い、その後[h(passwd1),rand1]Rkey,[h(passwd2),rand2]Rkeyを受信して[h(passwd1),rand1]Rkey,[h(passwd2),rand2]Rkeyの復号化(S61)を行うようにしてもよい。この場合でも、暗号化されたパスワード及び暗号化された乱数を受信するステップと、暗号化されたパスワード及び暗号化された乱数を復号化するステップとを備えていることになる。

【0072】【認証】パスワードを二つ利用する場合の認証方法を図1,4,5,6,7,8を用いて、説明する。認証に関しては、図1におけるクライアント15内の認証要求部19とサーバ27内の認証部30が動作し、図4は、図1の認証に関係する部分を抜粋したものである。

【0073】図4においてユーザは、IDcとAuthReqを入力部16に入力すると、これらの情報は認証要求部19に渡される。認証要求部19においてクライアント15は、ユーザのID(IDc)と認証要求AuthReqを通信部17を介してサーバ27に転送する。サーバ27は、通信部28においてAuthReqを含んだデータを受信すると、認証部30にデータを渡す。

【0074】次いで、認証部30内のCHALLENGE生成部30aにおいて、乱数情報CHALLENGEを生成しクライアント15に送信する。クライアント15は、CHALLENGEを受信すると、ユーザは、転送するパスワードの番号(1 or 2)と二つのパスワードを入力部16からクライアント15へ入力する。この場合は、パスワードを二つ利用し、passwd1を転送するので、n=1とpasswd1,passwd2を入力する。

【0075】次に、RESPONSE生成部19aは、入力されたパスワードとnを元に、パスワードとCHALLENGEからの乱数情報に暗号演算を施したものを作成してサーバ27へ送信する。サーバ27は、RESPONSEを受信すると、認証部30内のRESPONSE検証部30bにおいて、非公開パスワードファイル37bから、ハッシュ化されたパスワードを取り出し、RESPONSEを復号化する。復号化して得られた転送パスワードを検証することでクライアント15(ユーザ)を認証する。認証結果をANSWERとしてクライアント15に返す。以下に、CHALLENGE生成

21

部30a、RESPONSE生成部19a、RESPONSE検証部30bの詳細を説明する。

【0076】[CHALLENGE生成部30aの詳細]CHALLENGE生成部30aについて、図5を用いてさらに詳細に説明する。CHALLENGE生成部30aでは、ハッシュ化パスワード取得部38から、非公開パスワードファイル37bにあるIDcに該当するユーザのハッシュ化されたパスワードh(passwd1), h(passwd2)を取り出す。

【0077】乱数生成部39は、乱数challenge1, challenge2を生成する(S11)。challenge1は登録したパスワードのうちの一つを利用して認証を行う場合に用いる乱数情報であり、challenge2は登録した二つのパスワード両方を利用する場合に用いる乱数情報である。暗号化関数部35はchallenge1をh(passwd1)で暗号化し、[challenge1]h(passwd1)を出力する。次いで、暗号化関数部35はchallenge2をh(passwd2)で暗号化し、[challenge2]h(passwd2)を出力する。最後に、二つの暗号化結果を連結し、すなわち、CHALLENGE=[challenge1]h(passwd1), [challenge2]h(passwd2)をクライアントに対して送信する(S12)。challenge1, challenge2を暗号化して送るのは、後にパスワードの転送にchallenge1, challenge2が利用されるのでこれらを保護することで第三者に対してパスワードの推測攻撃を困難にするためである。

【0078】[ハッシュ化パスワード取得部38]ハッシュ化パスワード取得部38の動作を図6を用いて詳細に説明する。ハッシュ化パスワード取得部38は、非公開パスワードファイル37bと、masterkey 36と、復号化関数部34で構成される。

【0079】まず、復号化関数部34は、非公開パスワードファイル37bにおいてIDcで区別される登録情報の最後に記録されている[Rkey]masterkeyを、サーバ27が秘密に保持するmasterkey36を利用して復号化し、Rkeyを出力する。次に、復号化関数部34は、登録情報の[h(passwd1)]RkeyをRkeyにより復号化し、h(passwd1)を出力する。次いで、復号化関数部34は、登録情報の[h(passwd2)]RkeyをRkeyにより復号化しh(passwd2)を出力する。ハッシュ化パスワード取得部38は、h(passwd1)とh(passwd2)を出力する。

【0080】[RESPONSE生成部19aの詳細]RESPONSE生成部19aの動作を図7を用いて説明する。図4においてユーザからクライアント15へ入力された二つのパスワードpasswd1, passwd2と、転送したいパスワードの番号n(ここではpasswd1を転送するので、n=■1■を入力)は、入力部16を通じてRESPONSE生成部19aに渡される(S14, S15)。RESPONSE生成部19aにおいて、一方向性ハッシュ関数部21は、非転送パスワードpasswd2を入力として、h(passwd2)を出力する。

【0081】選択部200は、サーバ27から受信(S13)したCHALLENGEの内、入力されたパスワードの数

22

に対応した情報を選択する。この場合には、2つのパスワードが入力されたので、選択部200はここでCHALLENGEの二番目のデータである[challenge2]h(passwd2)を選択する。そして、選択した情報を復号化関数部25に対して出力する。復号化関数部25は、受信したCHALLENGEの二番目のデータである[challenge]h(passwd2)をh(passwd2)を用いて復号化し、challenge2を出力する。

【0082】次いで、乱数生成部22は、乱数nonceを生成する。暗号化関数部23は、一方向性ハッシュ関数部21から出力されたh(passwd2)を鍵としてnonceを鍵暗号化し、[nonce]h(passwd2)を出力する(S17)。又、xor関数部26は、passwd1、復号化関数部25から出力されたchallenge2、乱数生成部22から出力されたnonceについて排他的論理和をとり、challenge2@passwd1@nonceを出力する(S18)。

【0083】次いで、一方向性ハッシュ関数部21は、challenge2と■1■を入力として、h(challnge2, 1)を出力する。challenge2を利用する意味は、パスワードを2つ使うという意味で、“1”はそのうちpasswd1を転送するという意味である。最後に、これら三つの出力を連結し、RESPONSE=h(challnge2, 1), challenge2@passwd1@nonce, [nonce]h(passwd2)を出力する(S19)。

【0084】RESPONSEにおいては、passwd1はnonceとchallenge2の排他的論理和という形で保護され転送されるので、nonceとchallenge2が漏洩しない限りはpasswd1は漏洩しない。また、nonceはRESPONSEにおいてh(passwd2)を鍵として鍵暗号化されており、challenge2もCHALLENGEにおいてh(passwd2)により暗号化され保護されている。

【0085】さらに、認証においてパスワードを二つ利用し、第一番目のパスワードを転送することを示すh(challnge2, 1)を転送することで、第三者から転送するパスワード情報を秘匿することができる。乱数であるchallenge2を用いているため、h(challnge2, 1)は第三者からはランダムな情報に見え、CHALLENGEにおいてはchallenge2自体が暗号化されているのでchallenge2を知ることができず、第三者は転送するパスワードが一番目なのか二番目なのか、又、パスワードを一つだけ利用しているのか二つ利用しているのかを知ることができなくなっている。

【0086】[RESPONSE検証部30bの詳細]RESPONSE検証部30bの動作を図8を用いて詳細に説明する。サーバ27は、クライアント15からRESPONSEを受信する(S20)。そして、利用パスワード識別部40は、クライアント15から受信したRESPONSEの最初のデータがh(challnge2, 1)であることを確かめる(S21)。

(実際は、受信データの最初のデータがh(challnge1, 1), h(challnge1, 2), h(challnge2, 1), h(chall

23

enge 2, 2)のうちで、 $h(challenge\ 2, 1)$ になった場合に本実施の形態に示される動作が起る)。

【0087】 $h(challenge\ 1, 1)$ は、1つのパスワードを用いた認証であり、その認証に用いるパスワードは $passwd1$ であることを示し、 $h(challenge\ 1, 2)$ は、1つのパスワードを用いた認証であり、その認証に用いるパスワードは $passwd2$ であることを示す。 $h(challenge\ 2, 1)$ は、2つのパスワードを用いた認証であり、転送に用いるパスワードは $passwd1$ であることを示し、 $h(challenge\ 2, 2)$ は、2つのパスワードを用いた認証であり、転送に用いるパスワードは $passwd2$ であることを示す。

【0088】利用パスワード識別部40は、 $h(challenge\ 2, 1)$ の“challenge2”により、パスワードを二つ利用した認証であることを認識し、“1”により $passwd1$ が転送されてくることを認識する。

【0089】RESPONSE検証部30b以外はこの部分の意味を知ることはできないので、転送するパスワードに関する情報(いくつパスワードを利用しているのか、何番目のパスワードを転送しているのか)は第三者には漏洩しない。従って、パスワードの解析に対する情報を与えないことになる。

【0090】次に、ハッシュ化パスワード取得部38は、利用パスワード識別部40の認識結果に基づき、 $h(passwd1), h(passwd2)$ を得る(S22)。ここで、 $h(passwd1), h(passwd2)$ を得るのは、パスワードを2つ利用した認証であると利用パスワード識別部40が認識したからである。次に、復号化関数部34は、ハッシュ化パスワード取得部38から出力された $h(passwd2)$ を鍵として $[nonce]h(passwd2)$ を鍵復号化し、 $nonce$ を出力する(S23)。次いで、xor関数部41は、CHALLENGE生成時に生成したchallenge2とRESPONSEからのchallenge2@ $passwd1@nonce$ と、復号化関数部34の出力の $nonce$ を入力とし、 $passwd1$ を出力する(S24)。

【0091】一方向性ハッシュ関数部42は、xor関数部41から出力された $passwd1$ をハッシュ化し、 $h(passwd1)$ を出力する。比較部43は、一方向性ハッシュ関数部42から出力された $h(passwd1)$ と、ハッシュ化パスワード取得部38から得た $h(passwd1)$ とを比較し、一致すればクライアント15(ユーザ)を認証したとして“OK”を、一致しなければ認証しなかったとして“NG”をANSWER=OK/NGとして出力する(S25)。

【0092】この実施の形態における認証では、サーバから送信されるCHALLENGEに含まれた乱数challenge1, challenge2を用いることにより、認証に用いるパスワードの個数を指定するため、第三者によりRESPONSEを盗聴された場合であっても、第三者は乱数とのみ認識するだけでパスワードの個数をいくつに指定しているのかを知ることができない。例えば、第三者がクライアントから送信される複数のRESPONSEを盗聴したとしても、それ

24

ら複数のRESPONSEにおいて使用されるchallenge1又はchallenge2は、同一の値ではないので、複数のRESPONSEを比較しても、パスワードの個数をいくつに指定しているのかは分からない。

【0093】また、ユーザからの送信するRESPONSEにおいて $passwd1$ と乱数challenge2は排他的論理和がとられており、乱数challenge2が一種の暗号化に用いられるため、第三者による $passwd1$ の解読が困難となる。

【0094】さらに、RESPONSEにおいてクライアント内で生成した乱数nonceを用いて $passwd1$ と排他的論理和をとっているため、第三者による $passwd1$ の解読がさらに困難となる。さらにまた、クライアント内で生成した乱数nonceは、 $passwd2$ に基づく情報 $h(passwd2)$ をによって鍵暗号化されて送信されるため、クライアントからユーザに対して乱数nonceを送信する際に第三者に知られるのを防止できる。

【0095】さらにまた、この実施の形態においては乱数nonce、 $passwd1$ 、 $passwd2$ を用いた認証を行っているが、 $passwd2$ に基づく情報 $h(passwd2)$ は乱数nonceを鍵暗号化するためのパスワードとして使用されるので、実際にサーバ27に対して送信される情報量は、乱数nonce、 $passwd1$ の情報量となる。したがって、乱数nonce、 $passwd1$ 、 $passwd2$ を用いることで第三者による解読を困難にしつつ、送信する情報量が抑えられている。

【0096】また、この実施の形態においてはサーバ27は、クライアント15からRESPONSEとして、 $h(challenge\ 2, 1), challenge\ 2@passwd1@nonce, [nonce]h(passwd2)$ を受信するが、これらの情報を必ずしも一度に送信する必要はなく、まず、 $h(challenge\ 2, 1)$ をクライアント15から送信してサーバ27が受信し、その後challenge2@ $passwd1@nonce, [nonce]h(passwd2)$ をクライアント15から送信してサーバ27が受信するようにしてもよい。

【0097】(パスワード更新の概要)図1, 3, 9, 10, 11, 12を用いて、パスワードの更新方法を解説する。この実施の形態におけるパスワードの更新は、サーバ27において保持されている公開パスワードファイル37a、非公開パスワードファイル37bに格納されているハッシュ化されたパスワードを更新することをいう。以下、その方法を説明する。

【0098】パスワードの更新は図1において、クライアント15のパスワード更新要求部20とサーバ27のパスワード更新部31により実行され、図9は、図1のパスワードの更新に関係する部分を抜粋したものである。

【0099】ユーザがパスワードを更新を希望する場合、ユーザは入力部16を介してクライアント15に、IDcとパスワードの更新を示すRenewReqを入力すると、これらはパスワード更新要求部20に渡され、さらに通信部17はサーバ27に対して送信する。サーバ27の

25

パスワード更新部31は、IDcとRenewReqを通信部28介して受信すると、CHALLENGE生成部30aにおいて図5と同じ方法で乱数情報CHALLENGEを生成し(S31)、クライアント15へ送信する(S32)。

【0100】図15においてクライアント15は、通信部17を介してCHALLENGEを受信する(S33)と、ユーザは、入力部16を通じて、二つのパスワードpasswd1,passwd2、新しいパスワードpasswd3を入力する(S34)。これら3つのパスワードは、パスワード更新要求生成部20aに渡され、CHALLENGEを利用して3つのパスワードを暗号化したパスワード更新要求を出力する(S36)。通信部17はこの要求をサーバ27へ転送する。サーバ27は通信部28を介してクライアント15からのパスワード更新要求を受信すると、パスワード更新部31に渡す。

【0101】パスワード更新部31内のパスワード更新要求検証部31aは、パスワード更新要求を復号化、認証し、正しいクライアント(又はユーザ)ならば、新しいパスワードpasswd3を図3に示される非公開パスワードファイル37bと公開パスワードファイル37aにおいて登録・更新する。クライアント15は更新後の公開パスワードファイル37aを確認することで登録状況を確かめる。パスワード更新要求検証部31aが正しくないクライアントと判断した場合は、■NG■をクライアント15に対して送信する。以下に、パスワード更新要求生成部20a、パスワード更新要求検証部31aの詳細を説明する。

【0102】(パスワード更新要求生成部20a)パスワード更新要求部20で機能するパスワード更新要求生成部20aの動作を図10を用いて詳細に説明する。

【0103】ユーザは、入力部16を通じて、二つのパスワードpasswd1,passwd2、新しいパスワードpasswd3を入力する(S34)。これら3つのパスワードは、パスワード更新要求生成部20aに渡される。一方向性ハッシュ関数部21は、入力部16から渡されたpasswd1をハッシュ化しAh(passwd1)を出力する。

【0104】選択部200は、サーバ27から受信(S33)したCHALLENGEの内、更新対象となるパスワードに対応した情報を選択する(S35)。この場合には、passwd1を更新対象とするため[challenge1]h(passwd1)を選択する。そして、選択した情報を復号化関数部25に対して出力する。尚、passwd2を更新対象とする場合には、選択部200は[challenge2]h(passwd2)を選択して出力することになる。

【0105】次に、復号化関数部25は、選択部200から出力された[challenge1]h(passwd1)を、一方向性ハッシュ関数部21からの出力であるh(passwd1)を鍵として鍵復号化し、challenge1を出力する。

【0106】次いで、xor関数部26は、復号化関数部25からの出力であるchallenge1と入力部17から渡

26

されたpasswd1の排他的論理和をとり、challenge1@passwd1を出力する。

【0107】次いで、暗号化関数部23は、一方向性ハッシュ関数部21からの出力であるh(passwd1)を鍵として、xor関数部26から出力されるchallenge1@passwd1を鍵暗号化し、[challenge1@passwd1]h(passwd)を出力する。次に、一方向性ハッシュ関数部21は、入力部16から入力された新しいパスワードpasswd3をハッシュ化し、h(passwd3)を出力する。暗号化関数部23から出力された[challenge1@passwd1]h(passwd1)と、一方向性ハッシュ関数部21から出力されたh(passwd3)とは、連結され[challenge1@passwd1]h(passwd1),h(passwd3)となる。

【0108】次いで、乱数生成部22は乱数nonceを生成する。次いで、暗号化関数部23はnonceを利用して[challenge1@passwd1]h(passwd1),h(passwd3)を暗号化し、[(challenge1@passwd1)h(passwd1),h(passwd3)]nonceを出力する。

【0109】次に、一方向性ハッシュ関数部21は、入力部16から入力されたpasswd2をハッシュ化し、h(passwd2)を出力する。また、暗号化関数部23はh(passwd2)を用いてnonceを暗号化し、[nonce]h(passwd2)を出力する。

【0110】一方向性ハッシュ関数部21は、復号化関数部25からchallenge1を入力し、h(challenge1)を出力する。ここでh(challenge1)はpasswd1を更新することを示す。最後に一方向性ハッシュ関数部21から出力されたh(challenge1)と、暗号化関数部23から出力された[(challenge1@passwd1)h(passwd1),h(passwd3)]nonceと、暗号化関数部23から出力された[nonce]h(passwd2)とを連結してパスワード更新要求としてRESPONSEを出力する(S36)。

【0111】パスワード更新要求RESPONSEのh(challenge1)は、1番めのパスワードを更新することを示すが、第三者には一番目のパスワードを更新するのか二番目のパスワードを更新するのかは解らない。又、更新するハッシュ化パスワードh(passwd3)はnonceにより暗号化されており、又、nonceもh(passwd2)により暗号化されているので安全に転送される。

【0112】(パスワード更新要求検証部31a)パスワード更新部31で機能するパスワード更新要求検証部31aの動作を図11を用いて詳細に説明する。サーバ27はクライアントからRESPONSEを受信する(S37)。クライアント15からパスワード更新要求RESPONSEが通信部28を介して、パスワード更新部31に渡されると、パスワード更新要求検証部31aの更新パスワード識別部44が、RESPONSEの先頭のデータを見て、h(challenge1)であることを確認する(S38)。(実際は、受信データの最初のデータがh(challenge1), h(challenge2)のうちで、h(challenge1)になった場合に本

27

実施の形態に示される動作が起る）。この実施の形態では、更新パスワード識別部44は、 $h(challenge\ 1)$ によりpasswd1を更新することを認識する。

【0113】次に、図6と同じ方法で、ハッシュ化パスワード取得部38を利用して $h(passwd\ 1)$ と $h(passwd\ 2)$ を取り出す。次に、復号化関数部34は、ハッシュ化パスワード取得部38から出力された $h(passwd\ 2)$ を用いて、パスワード更新要求RESPONSEの $[nonce]h(passwd\ 2)$ を復号化し、nonceを出力する。さらに復号化関数部34は、nonceを用いて、パスワード更新要求RESPONSEの $[(challenge\ 1 @passwd\ 1)]h(passwd\ 1), h(passwd\ 3)]nonce$ を復号化し $[(challenge\ 1)@passwd\ 1]h(passwd\ 1), h(passwd\ 3)$ を出力する。

【0114】次いで、復号化関数部34はハッシュ化パスワード取得部38から出力された $h(passwd\ 1)$ を用いて、 $[(challenge\ 1)@passwd\ 1]h(passwd\ 1)$ を復号化し、 $challenge\ 1 @passwd\ 1$ を出力する。次いで、xor関数部41は、CHALLENGEを生成するときに生成したchallenge1と復号化関数部34から出力された $challenge\ 1 @passwd\ 1$ を入力とし排他的論理和を計算して、passwd1を出力する。一方向性ハッシュ関数部42はこのpasswd1を入力とし、 $h(passwd\ 1)$ を出力する。

【0115】比較部43は、一方向性ハッシュ関数部42からの出力結果とハッシュ化パスワード取得部38から得た $h(passwd\ 1)$ とを比較する（S39）。一致すれば、クライアント15（ユーザ）を正当に認証したとして、ハッシュ化パスワード更新部45により、公開パスワードファイル37aと非公開パスワードファイル37bの内容を図12の様に変更する（S310）。比較部43の結果が一致しなかったらば、■NG■を出力する。

【0116】この実施の形態における更新においては、サーバから送信されるCHALLENGEに含まれた乱数challenge1, challenge2を用いることにより、更新するパスワードを指定するため、第三者によりRESPONSEを盗聴された場合であっても、第三者は乱数とのみ認識するだけで、どのパスワードを更新するのかを知ることができない。例えば、第三者がクライアントから送信される複数のRESPONSEを盗聴したとしても、それら複数のRESPONSEにおいて使用されるchallenge1又はchallenge2は、同一の値ではないので複数のRESPONSEを比較することによりどのパスワードを更新しようとしているかを知ることはできない。

【0117】また、ユーザからの送信するRESPONSEにおいて更新対象を示すpasswd1と乱数challenge1の排他的論理和がとられ、かつ $h(passwd\ 1)$ で暗号化され、さらに、乱数nonceで $h(passwd\ 3)$ とともに暗号化されるため、第三者によるpasswd1の解読が困難となる。また、更新後のパスワードであるpasswd3はハッシュ化され、さらに乱数nonceで暗号化されるため、第三者によるpasswd3の解読が困難となる。さらに、クライアント

28

内で生成した乱数nonceは、passwd2により暗号化されて送信されるため、クライアントからユーザに対して乱数nonceを送信する際に第三者に知られるのを防止できる。

【0118】さらに、この実施の形態における認証では、2つのパスワードpasswd1とpasswd2の内、実際にサーバに転送するのは何れか一方のパスワードであり、他方のパスワードは暗号化するための秘密鍵として用いている。

10 【0119】尚、この実施の形態においては、CHALLENGE、RESPONSEを構成する各情報がハッシュ化、暗号鍵を用いた鍵暗号化、排他的論理和によって秘匿化されているが、必ずしもこれらの方法に限定されるものではない。

【0120】【ハッシュ化パスワード更新部45】ハッシュ化パスワード更新部45の動作を図12を用いて詳細に説明する。ハッシュ化パスワード更新部45は、上述のように比較部43によってクライアント15（又はユーザ）を正当に認証した場合に動作する。ハッシュ化パスワード更新部45は、暗号化関数部35と復号化関数部34と公開鍵パスワードファイル37aと、非公開パスワードファイル37bで構成される。

20 【0121】まず、復号化関数部34は、非公開パスワードファイル37a（更新前）内のIDcで区別されるユーザの登録情報において、最後に登録されている[Rkey]masterkeyをmasterkey36を用いて復号化し、Rkeyを出力する。次に、暗号化関数部35は、更新するハッシュ化パスワード $h(passwd\ 3)$ をRkeyを用いて暗号化し $[h(passwd\ 3)]Rkey$ を出力する。

30 【0122】ハッシュ化パスワード更新部45は、更新パスワード識別部44により、どのパスワードを更新するかを知ることができる。この実施の形態においてハッシュ化パスワード更新部45は、passwd1を更新することを認識する。そして、ハッシュ化パスワード更新部45は、公開パスワードファイル37aおよび非公開パスワードファイル37bに既に登録されている $(h(passwd\ 1))Rkey$ の代わりに暗号化関数部35から出力された $(h(passwd\ 3))Rkey$ を登録する。このような手順により、公開パスワードファイル37aと非公開パスワードファイル37bを図のように更新することができる（更新後で示されている）。

【0123】この実施の形態においては、登録要求としてRegReqを、認証要求としてAuthReqを、更新要求としてRenewReqをクライアントからユーザに対して送信するが、要求の種類を第三者に知られたくない場合には、これらRegReq、AuthReq、RenewReqについても秘匿化してもよい。また、この実施の形態における更新方法では、一方向性ハッシュ関数を用いて秘匿化している部分があるが、この機能を秘密鍵暗号によっても実現することも

50 できる。

29

【0124】この実施の形態においては、クライアントとサーバでの処理について具体的に説明しているが、必ずしもクライアント、サーバのみに適用されるものではない。以降の実施の形態についても同様である。

【0125】この実施の形態においては、クライアント15からサーバ27に対して $h(challenge\ 1, [[challenge\ 1 @passwd\ 1]h(passwd\ 1), h(passwd\ 3)]nonce, [nonce]h(passwd\ 2)]$ を受信するが、これらの情報を必ずしも一度に送信する必要はなく、まず $h(challenge\ 1)$ をクライアント15から送信してサーバ27が受信し、その後 $[[challenge\ 1 @passwd\ 1]h(passwd\ 1), h(passwd\ 3)]nonce, [nonce]h(passwd\ 2)]$ をクライアント15から送信してサーバ27が受信するようにしてもよい。

【0126】実施の形態2、実施の形態1においては、パスワードを二つ用いる認証方法について説明した。実施の形態2では、パスワードを一つだけ利用した場合の認証方法を記す。パスワードの登録、更新は実施の形態1と同じである。この実施の形態における認証方法により、ユーザは、サーバに登録した二つのパスワードの内、覚えている方のパスワードを多用することができる。

【0127】この認証方法は、図4において、ユーザがクライアント15に入力する情報を、認証に利用するパスワード一つ（ここではpasswd1）とその番号n（passwd1ならば1）とし、RESPONSE生成部19aの動作を図13に示すように、RESPONSE検証部30bの動作を図14に示すように置き換えることで実現される。なお、RESPONSE生成部19a、RESPONSE検証部30bの構成は実施の形態1と同じである。

【0128】[図13の詳細]実施の形態2におけるRESPONSE生成部19aの動作を図13を用いて説明する。図4においてユーザによりクライアント15へ入力されたパスワード（ここではpasswd1）、転送したいパスワードの番号nは（ここではpasswd1を転送するので、n=■1■を入力）は、入力部16を通じて図13で示されるRESPONSE生成部19aに渡される。

【0129】次に、RESPONSE生成部19aにおいて、一方向性ハッシュ関数部21は、パスワードpasswd1を入力とし $h(passwd\ 1)$ を出力する。さらに、選択部200は、受信したCHALLENGEの内、認証に用いるパスワードの個数に対応した情報を選択する。この場合には1つのパスワードを用いた認証を行うので、CHALLENGEの一番目のデータである $[challenge\ 1]h(passwd\ 1)$ を選択する。尚、パスワードを2つ用いて認証を行う場合には、CHALLENGEの内、 $[challenge\ 2]h(passwd\ 2)$ を選択することになる。そして、選択した情報を復号化関数部25に対して出力する。復号化関数部25は、受信したCHALLENGEの一番目のデータである $[challenge\ 1]h(passwd\ 1)$ を、 $h(passwd\ 1)$ で復号化し、challenge1を出力する。ここで、

30

【0130】次に乱数生成部22は、乱数nonceを生成する。次いで暗号化関数部23は、一方向性ハッシュ関数部21から出力された $h(passwd\ 1)$ を用いてnonceを暗号化し、 $[nonce]h(passwd\ 1)$ を出力する。次に、xor関数26は入力されたpasswd1、復号化関数部25から出力されたchallenge1、nonceを入力として排他的論理和を計算し、 $challenge\ 1 @passwd\ 1 @nonce$ を出力する。

【0131】次いで、一方向性ハッシュ関数部21は、復号化関数部25から出力されたchallenge1と■1■を入力として、 $h(challnge\ 1, 1)$ を出力する。 $h(challnge\ 1, 1)$ における“challnge1”は、パスワードを1つ用いた認証であることを示し、 $h(challnge\ 1, 1)$ における“1”は、使用するパスワードはpasswd1であることを示す。

【0132】最後に、一方向性ハッシュ関数部21から出力された $h(challnge\ 1, 1)$ と、xor関数26から出力された $challenge\ 1 @passwd\ 1 @nonce$ と、暗号化関数部23から出力された $[nonce]h(passwd\ 1)$ を連結し、 $RESPONSE=h(challnge\ 1, 1), challenge\ 1 @passwd\ 1 @nonce, [nonce]h(passwd\ 1)$ を出力する。

【0133】[図14の詳細]実施の形態2におけるRESPONSE検証部30bの動作を図14を用いて詳細に説明する。サーバ27がクライアント15からRESPONSEを受信すると、RESPONSEは通信部28を介して図14で示されるRESPONSE検証部30bに渡される。まず、利用パスワード識別部40は、受信データRESPONSEの先頭データが、 $h(challnge\ 1, 1)$ であることを確認する（実際は、受信データの最初のデータが $h(challnge\ 1, 1)$ 、 $h(challnge\ 1, 2)$ 、 $h(challnge\ 2, 1)$ 、 $h(challnge\ 2, 2)$ ）のうちで、 $h(challnge\ 1, 1)$ になった場合に本実施の形態に示される動作が起る）。この実施の形態において利用パスワード識別部40は、RESPONSEの先頭データ $h(challnge\ 1, 1)$ の“challnge1”により、パスワードを1つ用いた認証であることを認識し、“1”により、使用するパスワードはpasswd1であることを認識する。

【0134】ハッシュ化パスワード取得部38は、利用パスワード識別部40による認識結果を基に、ユーザのID(IDc)に対応した $h(passwd\ 1)$ を取り出す。この実施の形態において、 $h(passwd\ 1)$ を取り出すのは、利用パスワード認識部40が、使用するパスワードをpasswd1であると認識したからである。尚、利用パスワード認識部40が、使用するパスワードをpasswd2と認識した場合には、ハッシュ化パスワード取得部38は $h(passwd\ 2)$ を取り出すことになる。次いで、復号化関数部34は、ハッシュ化パスワード取得部38から出力された $h(passwd\ 1)$ を用いてRESPONSEの $[nonce]h(passwd\ 1)$ を復号化し、nonceを出力する。

【0135】次に、xor関数部41は、nonceとRESPONSEからの $challenge\ 1 @passwd\ 1 @nonce$ 、CHALLENGEの生成

31

時に生成したchallenge 1を入力とし、passwd 1を出力する。一方性ハッシュ関数部42は、xor関数部41から出力されたpasswd 1をハッシュ化して出力する。比較部43は、一方性ハッシュ関数部42からの出力結果と、ハッシュ化パスワード取得部38から得たh(passwd 1)とを比較する。両者が一致すれば、クライアント15(又はユーザ)を正当に認証したとして■OK■を、両者が一致しない場合は正当ではないとして■NG■をANSWER=OK/NGとして出力する。

【0136】この実施の形態における認証は、登録した2つのパスワードの内、ユーザが指定したいずれか一方のパスワードを用いて認証することができるため、ユーザにとって利便性が高い。また、パスワードを2つ用いた認証でのRESPONSEも、パスワードを1つ用いた認証でのRESPONSEも、同じ情報量となるため、第三者がRESPONSEの情報量を手掛かりとして、認証に使用するパスワードの数を推測することを防止できる。また、パスワードを2つ用いた認証の場合でも、パスワードを1つ用いた認証の場合でも、クライアントおよびサーバは、ほとんど同じ処理で対応することができるため有効である。

【0137】また、第三者がパスワードの解読を行う場合には、クライアント15からサーバ27に対して送信される情報を経続して盗聴することが想定される。しかし、この実施の形態における認証方法の場合、パスワードを1つ用いた認証とパスワードを2つ用いた認証とをクライアントの利用者側で選択的に変更できるため、第三者が盗聴中に、認証に使用するパスワードの個数が変更されることにより第三者はパスワードをいくつ用いた認証なのかを特定できなくなる。よって、第三者はパスワード解読の手掛かりを得ることが困難になる。

【0138】実施の形態3. 実施の形態3では、実施の形態1において登録した2つのパスワードの内、どちらかのパスワードを忘れてしまった場合に、忘れた方のパスワードを更新する方法を示す。実施の形態3では、登録したpasswd 1, passwd 2の内、passwd 1を覚えていてpasswd 2を忘れた場合に、passwd 2を新しいパスワードpasswd 3に更新する方法について説明する。

【0139】図9において、ユーザは、クライアント15に、覚えているパスワード(ここでは、passwd 1)と、新しいパスワードpasswd 3、パスワードを失忘したこと示す0を入力する。この実施の形態におけるパスワードの更新は、クライアント15におけるパスワード更新要求生成部20aと、サーバ27におけるパスワード更新要求検証部31aによって行われる。

【0140】パスワード更新要求生成部20aの動作を図15に、パスワード更新要求検証部31aの動作を図16に示す。なお、パスワード更新要求生成部20aとパスワード更新要求検証部31aの構成は実施の形態1と同じである。

【0141】[パスワード更新要求生成部20aの動作

32

(図15)]実施の形態3におけるパスワード更新要求生成部20aの動作を図15を用いて説明する。図9において、ユーザによりクライアント15へ入力されたpasswd 1、新しいパスワード(更新パスワード)passwd 3、0、は入力部16を介して図15で示されるパスワード更新要求生成部20aに渡される。パスワード更新要求生成部20aでは、一方性ハッシュ関数部21はユーザから入力されたpasswd 1を入力としh(passwd 1)を出力する。

10 【0142】さらに、選択部200は、受信したCHALLENGEの中から、入力されたパスワードに対応した情報を選択する。この場合には、passwd 1が入力されたため、CHALLENGEの[challenge 1]h(passwd 1)を選択する。尚、入力されたパスワードがpasswd 2の場合には、[challenge 2]h(passwd 2)が選択されることになる。そして、選択部200は、選択した情報を復号化関数部25に対して出力する。次に、復号化関数部25は、CHALLENGEの[challenge 1]h(passwd 1)を一方性ハッシュ関数部21から出力されたh(passwd 1)を用いて復号化し、challenge 1を出力する。

【0143】次いで、xor関数部26は、復号化関数部25から出力されたchallenge 1と、ユーザにより入力されたpasswd 1の排他的論理和をとり、challenge 1@passwd 1を出力する。

【0144】暗号化関数部23は、一方性ハッシュ関数部21から出力されたh(passwd 1)を利用してxor関数部26から出力されたchallenge 1@passwd 1を暗号化し、[challenge@passwd 1]h(passwd 1)を出力する。次に、一方性ハッシュ関数部21は、ユーザにより入力された新しいパスワードpasswd 3をハッシュ化してh(passwd 3)を出力する。一方性ハッシュ関数部21から出力されたh(passwd 3)は、暗号化関数部23から出力された[challenge@passwd 1]h(passwd 1)と連結され、[challenge@passwd 1]h(passwd 1), h(passwd 3)となる。

【0145】次いで、乱数生成部22は、乱数nonceを生成し、暗号化関数部23はnonceを利用して[challenge@passwd 1]h(passwd 1), h(passwd 3)を暗号化し、[[challenge@passwd 1]h(passwd 1), h(passwd 3)]nonceを出力する。また、暗号化関数部23は、一方性ハッシュ関数部21から出力されたh(passwd 1)を用いてnonceを暗号化し、[nonce]h(passwd 1)を出力する。

【0146】次に、一方性ハッシュ関数部21は、復号化関数部25から出力されたchallenge 1と、ユーザにより入力された0とから、h(challenge 1, 0)を出力する。最後に、一方性ハッシュ関数部21から出力されたh(challenge 1, 0)と、暗号化関数部23から出力された[[challenge 1@passwd 1]h(passwd 1), h(passwd 3)]nonceと、暗号化関数部23から出力された[nonce]h(passwd 1)とを連結し、パスワード更新要求としてRES

PONSEを出力する。

【0147】この実施の形態においては、サーバから送信されたCHALLENGEに含まれた乱数challenge1を用い、 $h(challenge1, 0)$ として送信するので、どのパスワードを覚えているのかをサーバに知らせている。したがって、第三者がRESPONSEを盗聴したとしても、乱数としか認識できず、よってどのパスワードを更新するのかを知ることができない。また、入力したパスワードpasswd1と更新後のパスワードpasswd3は、クライアントで生成された乱数nonceによって暗号化されるため、第三者はpasswd1、passwd3の解読が困難である。また、サーバにおいては、乱数challenge1若しくはchallenge2が返ってくることで、1つの情報で、正当なクライアントであることが認識できるとともに、どのパスワードを更新するのかを知ることができる。

【0148】[パスワード更新要求検証部31a(図16)]実施の形態3におけるパスワード更新要求検証部31aの動作を図16を用いて説明する。図9において、サーバ27がクライアント15から通信部28を介してパスワード更新要求を受信すると、図16のパスワード更新要求検証部31aの更新パスワード識別部44が、受信データRESPONSEの先頭のデータを見て、 $h(challenge1, 0)$ であることを確認する(実際は、受信データの最初のデータが $h(challenge1, 0)$ 、 $h(challenge2, 0)$ のうちで、 $h(challenge1, 0)$ になった場合に本実施の形態に示される動作が起る)。更新パスワード識別部44は、 $h(challenge1, 0)$ の“challenge1”により現在知っているパスワードがpasswd1であることを認識し、“0”によりもう一つのパスワードpasswd2を現在所持していない(忘れた等)ことを認識する。

【0149】ハッシュ化パスワード取得部38は、更新パスワード識別部44の識別結果により、図6に示したのと同様の方法によりユーザーのID(IDc)に対応する $h(passwd1)$ を取り出す。次に、復号化関数部34はハッシュ化パスワード取得部38によって取り出した $h(passwd1)$ を用いて、パスワード更新要求RESPONSEの[nonce] $h(passwd1)$ を復号化し、nonceを得る。

【0150】次に、復号化関数部34は、nonceを用いて、パスワード更新要求RESPONSEの[[challenge1@passwd1] $h(passwd1)$, $h(passwd3)$]nonceを復号化し[[challenge1]@passwd1] $h(passwd1)$, $h(passwd3)$ を出力する。次いで、復号化関数部34は、ハッシュ化パスワード取得部38によって取り出した $h(passwd1)$ を用いて[challenge1@passwd1] $h(passwd1)$ を復号化し、challenge1@passwd1を出力する。

【0151】次にxor関数部41は、CHALLENGEを生成するときに生成したchallenge1と、challenge1@passwd1の排他的論理和をとり、passwd1を出力する。次いで、一方向性ハッシュ関数部42は、xor関数部41から出力されたpasswd1をハッシュ化し、 $h(passwd1)$ を

出力する。

【0152】次に、比較部43は、一方向性ハッシュ関数部42からの出力結果と、ハッシュ化パスワード取得部38から取り出した $h(passwd1)$ とを比較する。両者が一致すれば、クライアント15(又はユーザ)を正当に認証したとして、ハッシュ化パスワード更新部45が公開パスワードファイル37aと非公開パスワードファイル37bの内容を更新する。両者が一致しなければ、比較部43はNGを出力する。

10 【0153】ハッシュ化パスワード更新部45は、比較部43によってクライアント15(又はユーザ)を正当に認証した場合に動作する。更新方法は、公開パスワードファイル37aおよび非公開パスワードファイル37bにおける[[$h(passwd2)$]]Rkeyを[[$h(passwd3)$]]Rkeyに変更する。変更した後に公開パスワードファイル37aを公開し、クライアント15(又はユーザ)はこれを見てパスワードが更新されていることを確認する。

【0154】passwd2を覚えていて、passwd1を忘れた場合は、図15におけるpasswd1をpasswd2に、challenge1をchallenge2に置き換える。出力を $h(challenge2, 0)$, [[challenge2@passwd2] $h(passwd2)$, $h(passwd3)$]nonce, [nonce] $h(passwd2)$ とする。以降、図16においてpasswd1をpasswd2に、challenge1をchallenge2に置き換えて、同様の処理を行う。安全性を高めるならば、passwd1をpasswd3に更新した後で、passwd2を別のパスワードに更新すれば良い。

【0155】実施の形態4. 実施の形態1において、サーバ27がクライアント15(又はユーザ)を認証した結果をANSWER=OK/NGと返しているが、このような場合には、第三者がクライアントに対してANSWER=OKの信号を送信し、その応答としてクライアントが送信する情報を第三者が盗み出すことができるという問題がある。この実施の形態においては■OK■の代わりにサーバ27は、ANSWER= $h(challenge2, nonce)$ を返す。

【0156】クライアント15はサーバ27からANSWER= $h(challenge2, nonce)$ を受信すると、CHALLENGEから得たchallenge2とRESPONSE生成時に生成したnonceを一方向性ハッシュ関数部21に入力し、ハッシュ化する。一方向性ハッシュ関数部21によるハッシュ化の出力とANSWERとを比較して、両者が一致すればクライアント15(又はユーザ)はサーバ27に認証されたと判断する。なぜならば、正しい $h(challenge2, nonce)$ を生成できるのはハッシュ化されたパスワードを所持できるサーバ27だけであるからである。challenge2も、nonceもネットワーク上を転送されるときは暗号化されているので、第三者がこれらの情報を知ることはできない。従って、 $h(challenge2, nonce)$ を生成することはできない。

【0157】この実施の形態においては、ANSWERを構成する情報から、ANSWERが正当なサーバ27からの返答であるか否かを認識できる。尚、実施の形態2において

35

も、サーバ27はクライアント15に対してユーザが選択したchallenge1とnonceのハッシュ値ANSWER=h(challenge1,nonce)を返せば同じ効果が得られる。

【0158】実施の形態5。実施の形態5では、実施の形態1,2,3において、公開パスワードファイル37aの安全性を高める一手法を説明する。或ユーザAが、クライアント15を介してパスワードの登録・或いは更新を行い、サーバ27が即座に登録・更新した公開パスワードファイル37aを公開したとする。

【0159】ユーザA(又はクライアント15)の転送データを盗聴している悪者がいた場合、転送データがパスワードの登録要求或いは更新要求であったと分かると、公開パスワードファイル37aの変化分をユーザAのパスワードデータが登録或いは更新された影響としてとらえ、変化した情報をパスワードの解析に役立てる可能性がある。

【0160】実施の形態5では、実施の形態1,2,3において、公開パスワードファイル37aの公開のタイミングを周期的にすることで悪者が適切な判断をできなくなる。又、パスワードの登録時にランダムなダミー情報を公開パスワードファイル37aに混入することにより、悪者の判断の基準を搅乱し、パスワードの解析を防止する。具体的には、公開パスワードファイル37aに、乱数等から構成されたダミー情報を複数行登録しておき、公開のタイミングに応じて、このダミー情報の内容を変更する。

【0161】このような方法により、公開パスワードファイルが公開された場合に、更新された内容を第三者に知られるのを防止できる。

【0162】実施の形態6。実施の形態6では、実施の形態1に示した認証方法においてさらにパスワードのより安全な転送を実現する手法を説明する。

【0163】図4のCHALLENGE生成部において、出力をC=CHALLENGE=[challenge2]h(passwd1), [challenge1]h(passwd2)となるようにする。図4のRESPONSE生成部においては、このCHALLENGEを復号化し、RESPONSEをRESPONSE=h(challenge2,1), challenge2@passwd1@nonce, [nonce]h(passwd2)となるように計算する。以降の手順は実施の形態1と同じである。

【0164】この様にすることで、万が一h(passwd2)或いはpasswd2が漏洩したとしても、攻撃者は直接passwd1或いはh(passwd1)を知ることはできない。なぜなら、h(passwd2)を利用して[nonce]h(passwd2)を復号化し、nonceを得て、このnonceでRESPONSEの二番目の情報challenge2@passwd1@nonceの排他的論理和をとりchallenge2@passwd1を得たとする。

【0165】しかし、passwd1を知るためににはchallenge2が解る必要がある。攻撃者は、CHALLENGE=[challenge2]h(passwd1), [challenge1]h(passwd2)における[challenge2]h(passwd1)と、RESPONSEにおけるchall

36

nge2@passwd1の二つの情報から、passwd1とchallenge2の組み合わせをこの二つの情報に当てはまるよう検査しなくてはならない。

【0166】この実施の形態のようにCHALLENGEを構成することにより、第三者による解読をより困難にすることができる。

【0167】

【発明の効果】第1、第9の発明においては、第1処理装置において公開した場合でも、第2処理装置において

10 生成された任意情報によって暗号化されたパスワードが公開されるので、第3者は公開された情報からパスワードを解読することが困難となる。一方、第2処理装置側では、入力したパスワードが第1処理装置に正常に登録されたか否かを確認できる。

【0168】第2、第10の発明においては、第2処理装置側では、第1処理装置において生成された複数の任意情報のいずれかを選択することによって、パスワードをいくつ用いた認証を行うのかを第1処理装置に対して知らせるため、利用者はパスワードをいくつ用いて認証するのかを選択可能になって便利であり、第3者はいくつのパスワードを用いて認証を行っているのかを解読するのが困難となる。

【0169】第3の発明においては、上記第1受信ステップにおける複数の任意情報として乱数を用いるため、第3者はいくつのパスワードを用いて認証を行っているのかを解読するのがよりいっそう困難となる。

【0170】第4の発明においては、上記第2送信ステップは、上記入力された入力パスワードの数にかかわらず、上記入力パスワードを一定の情報量に変換して送信するため、第3者が情報量の大きさを手掛かりにパスワードをいくつ用いた認証を行っているのかを認識することを防止できる。

【0171】第5、第11の発明においては、第2処理装置では、入力された第1パスワード及び第2パスワードのいずれかを所定情報を鍵暗号化するための鍵暗号化用パスワードとして使用し、第2パスワード自体は第1処理装置に送信しないので第2パスワード分の送信情報量を削減することができ、かつ第三者にとっては第2パスワードを用いることにより解読が困難となる。

40 【0172】第6の発明においては、上記第2処理装置側の処理として、乱数を生成する乱数生成ステップを有し、上記パスワード暗号化ステップは、上記指定された送信パスワードを上記生成された乱数を用いて暗号化するため、第3者による送信パスワードの解読がより困難となる。

【0173】第7、第12の発明においては、第2処理装置側では、第1処理装置において生成された複数の任意情報のいずれかを選択することによって、どのパスワードを更新するのかを第1処理装置に対して知らせるため、第3者はどのパスワードが更新されるのかを解読す

るのが困難となる。

【0174】第8の発明においては、上記第1処理装置に登録された登録パスワードの更新は、上記第1処理装置に登録された複数のパスワードの内、任意の登録パスワードについて更新可能であるため、例えば利用者が複数のパスワードの内、一部のパスワードを忘れてしまった場合などにこの忘れたパスワードを新しいパスワードに更新することができる。したがって、利用者にとって便利である。

【0175】

【図面の簡単な説明】

【図1】 この発明の実施の形態1におけるクライアント-サーバー認証システムの構成図である。

【図2】 この発明の実施の形態1における、ユーザのクライアントを介してのサーバへのパスワード登録の方法を示す図である。

【図3】 この発明の実施の形態1における、ユーザのパスワードの登録に関係するファイルを示す図である。

【図4】 この発明の実施の形態1における、クライアント(ユーザ) - サーバ間での認証方法を示す図である。

【図5】 図4におけるサーバ27のCHALLENGE生成部30aを示す図である。

【図6】 図5におけるハッシュ化パスワード取得部38を示す図である。

【図7】 図4におけるクライアント15のRESPONSE生成部19aを示す図である。

【図8】 図4におけるサーバ27のRESPONSE検証部30bを示す図である。

【図9】 この発明の実施の形態1におけるクライアント15を介したユーザのパスワードの更新方法を示す図である。

【図10】 図9におけるクライアント15のパスワード更新要求生成部20aを示す図である。

【図11】 図9におけるサーバ27のパスワード更新要求検証部31aを示す図である。

【図12】 図11におけるハッシュ化パスワード更新部45を示す図である。

【図13】 実施の形態2における図4中のクライアント

15のRESPONSE生成部19aを示す図である。

【図14】 実施の形態2における図4中のクライアント15のRESPONSE検証部30bを示す図である。

【図15】 実施の形態3における図9内に表されるパスワード更新要求生成部20aを示す図である。

【図16】 実施の形態3における図9内に表されるパスワード更新要求検証部31aを示す図である。

【図17】 従来のクライアント-サーバ間のパスワードベースの認証技術であるPAP方式を示す図である。

10 【図18】 従来のクライアント-サーバ間のパスワードベースの認証技術であるCHAP方式を示す図である。

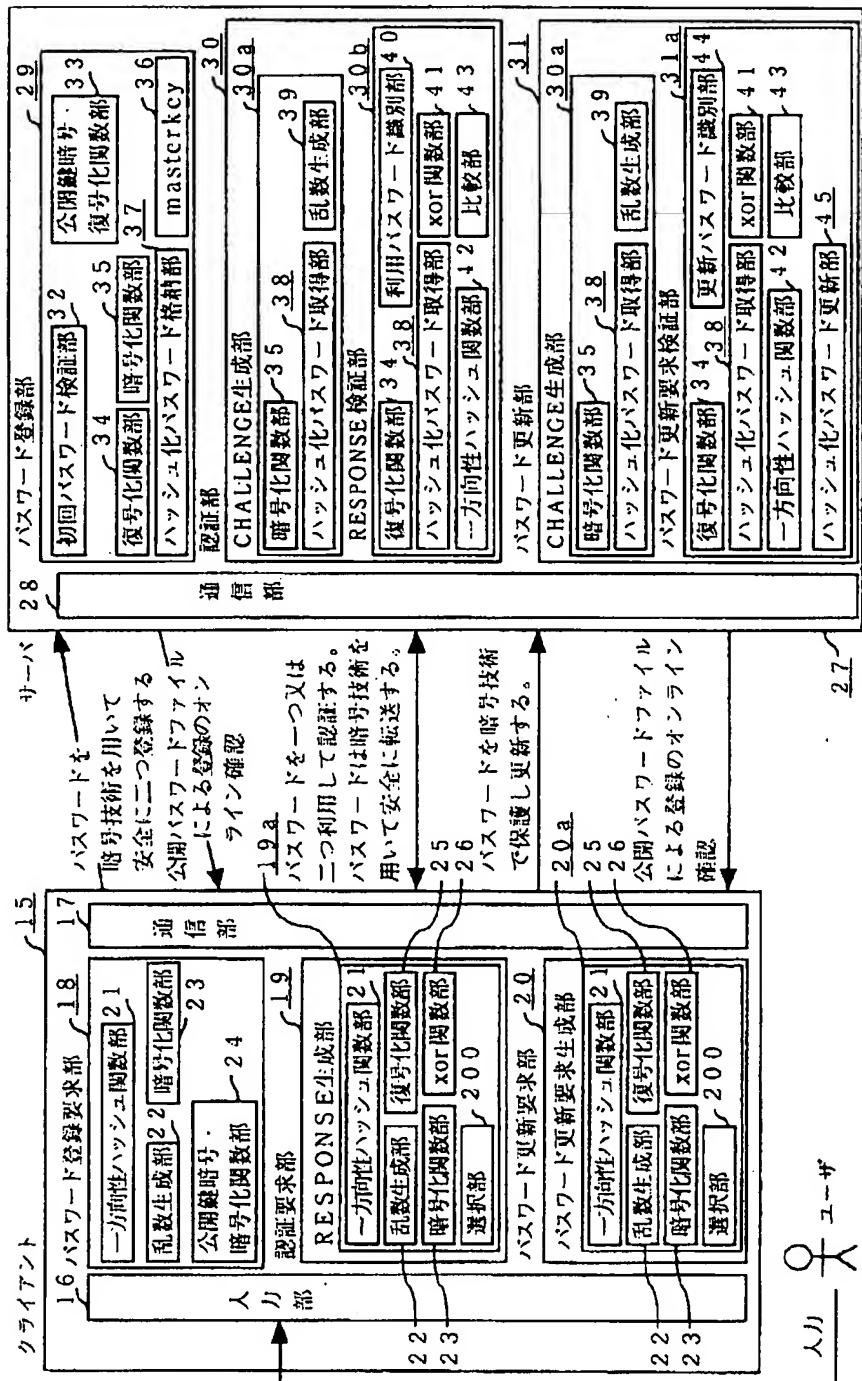
【図19】 従来の利用者確認方式を示す図である。

【符号の説明】

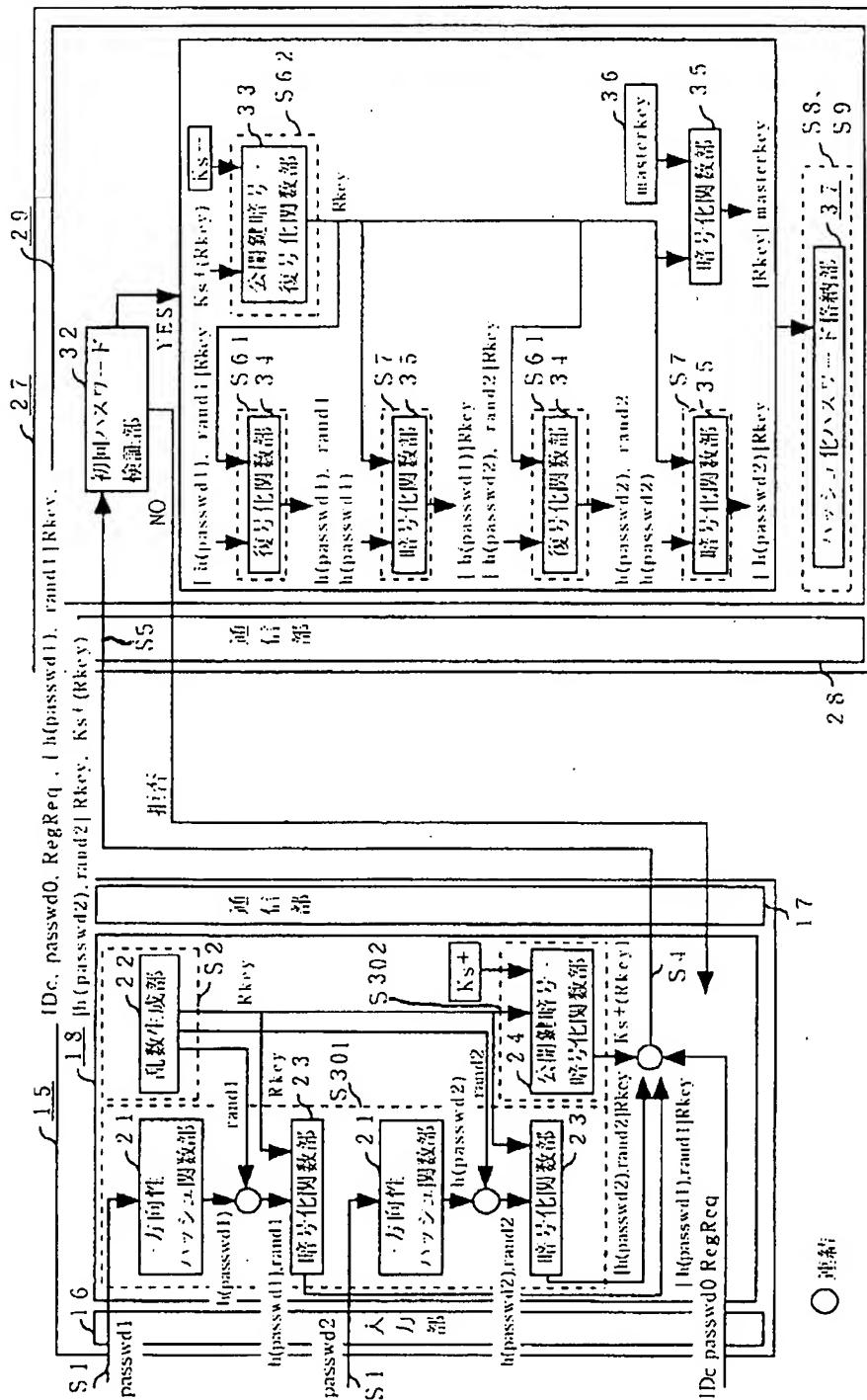
1 クライアント(PAP)、2 サーバ(PAP)、3 パスワードファイル(PAP)、4 パスワードファイル検索部(PAP)、5 暗号化部、6 比較部、7 クライアント(CHAP)、8 一方向性ハッシュ関数部(CHAP)、9 サーバ(CHAP)、10 乱数生成部、11 パスワードファイル(CHAP)、12 パスワードファイル検索部(CHAP)、13 一方向性ハッシュ関数部(CHAP)、14 比較部(CHAP)、15 クライアント、16 入力部、17 通信部、18 パスワード登録要求部、19 認証要求部、19a RESPONSE生成部、20 パスワード更新要求部、20a パスワード更新要求生成部、21 一方向性ハッシュ関数部、22 乱数生成部、23 暗号化関数部、24 公開鍵暗号・暗号化関数部、25 復号化関数部、26 xor関数部、27 サーバ、28 通信部、29 パスワード登録部、30 認証部、30a CHALLENGE生成部、30b RESPONSE検証部、31 パスワード更新部、31a パスワード更新要求検証部、32 初回パスワード検証部、33 公開鍵暗号・復号化関数部、34 復号化関数部、35 暗号化関数部、36 masterkey、37 ハッシュ化パスワード格納部、37a 公開パスワードファイル、37b 非公開パスワードファイル、38 ハッシュ化パスワード取得部、39 乱数生成部、40 利用パスワード識別部、41 xor関数部、42 一方向性ハッシュ関数部、43 比較部、44 更新パスワード識別部、45 ハッシュ化パスワード更新部、200 選択部。

20 30 31 32 33 34 35 36 37 37a 38 39 40 41 42 43 44 45 200

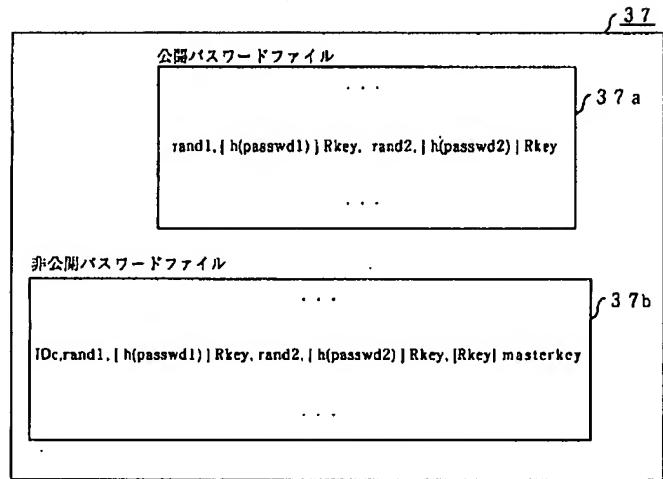
【図1】



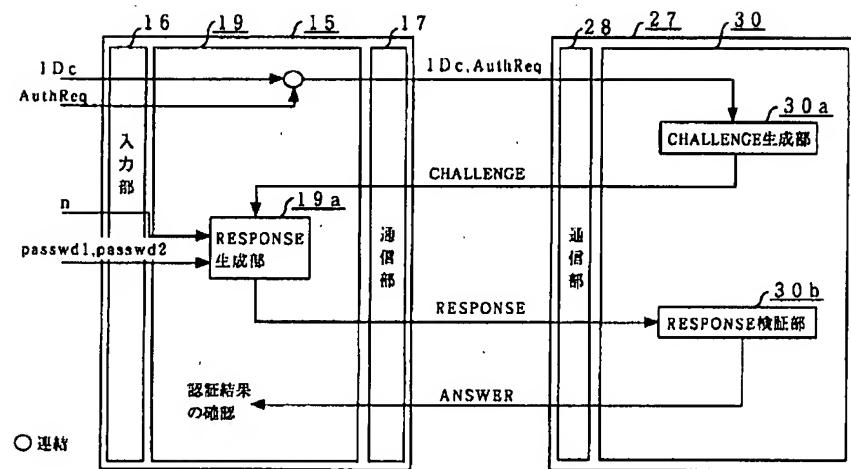
【図2】



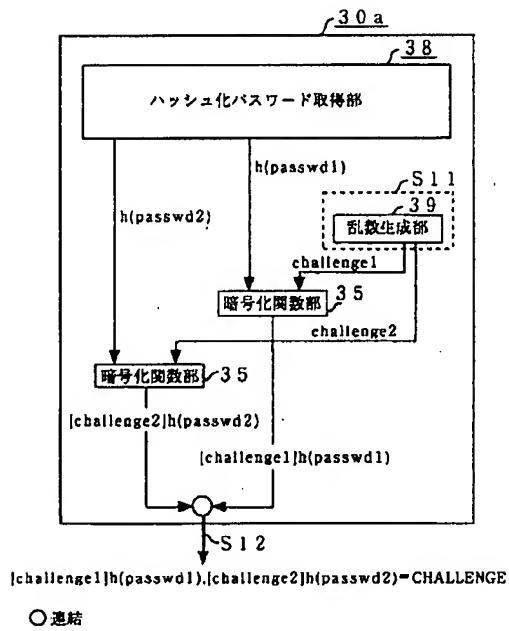
【図3】



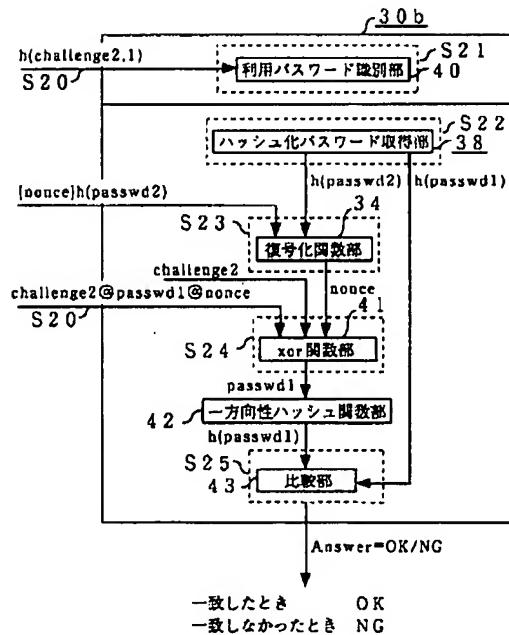
【図4】



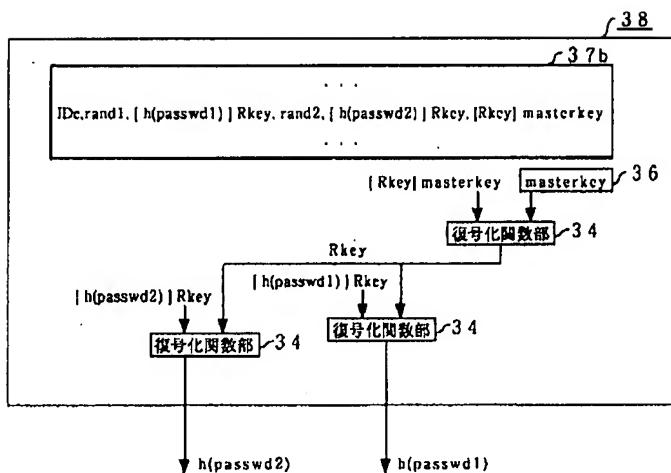
【図5】



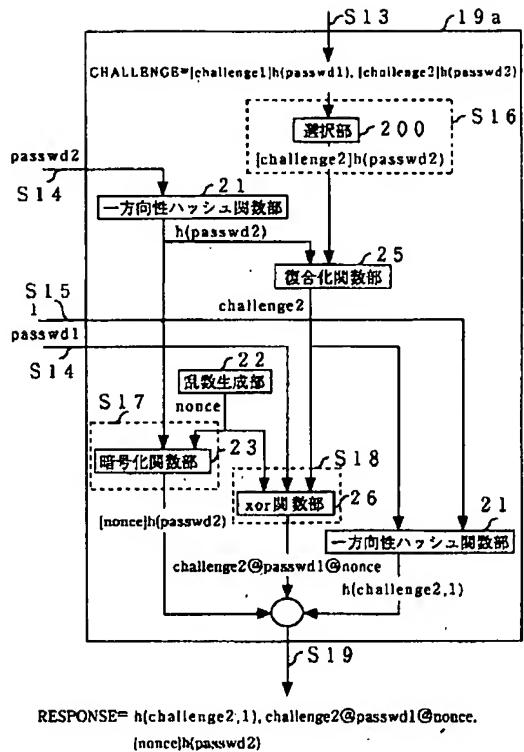
【図8】



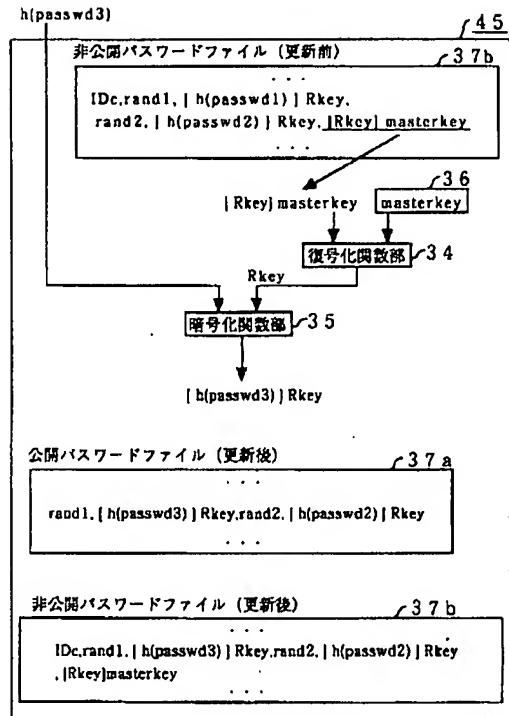
【図6】



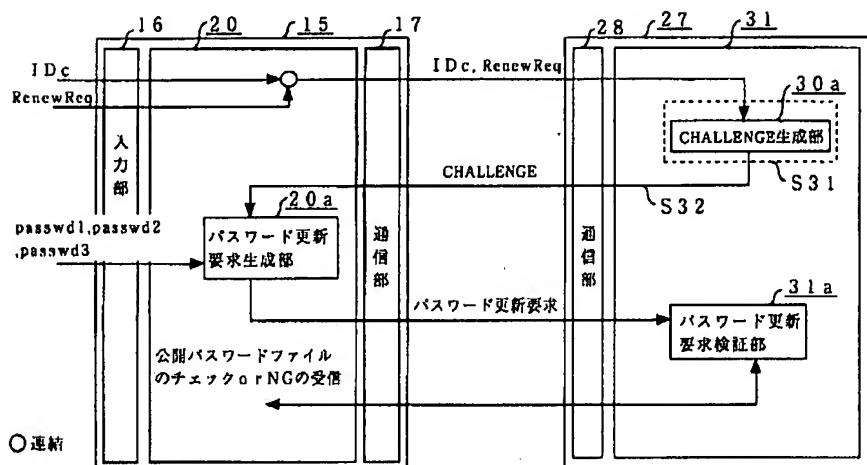
【図7】



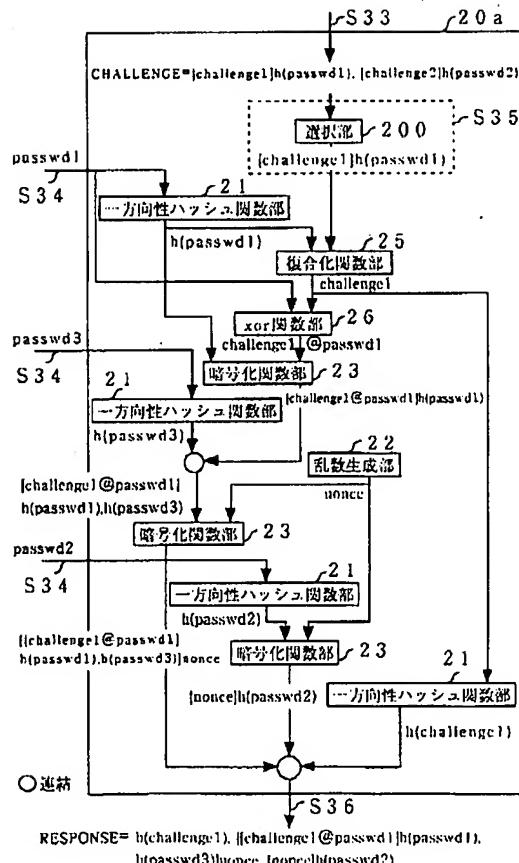
【図12】



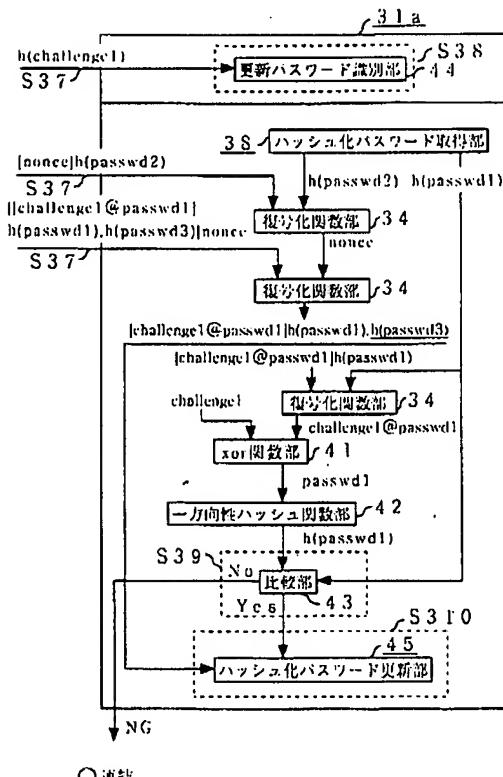
【図9】



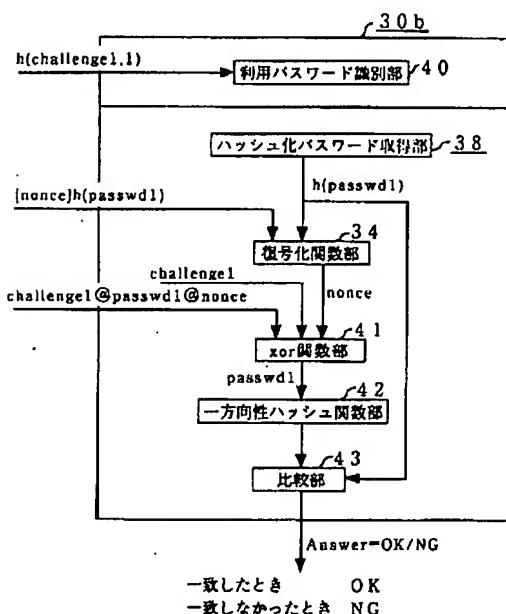
【図10】



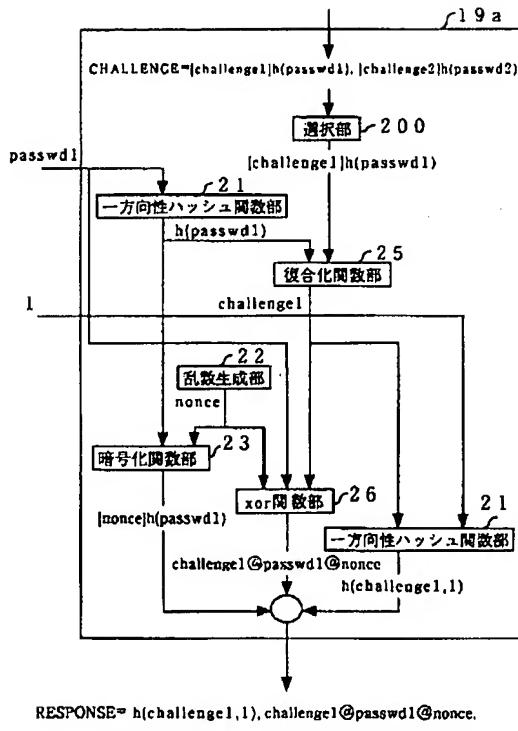
【図11】



【図14】

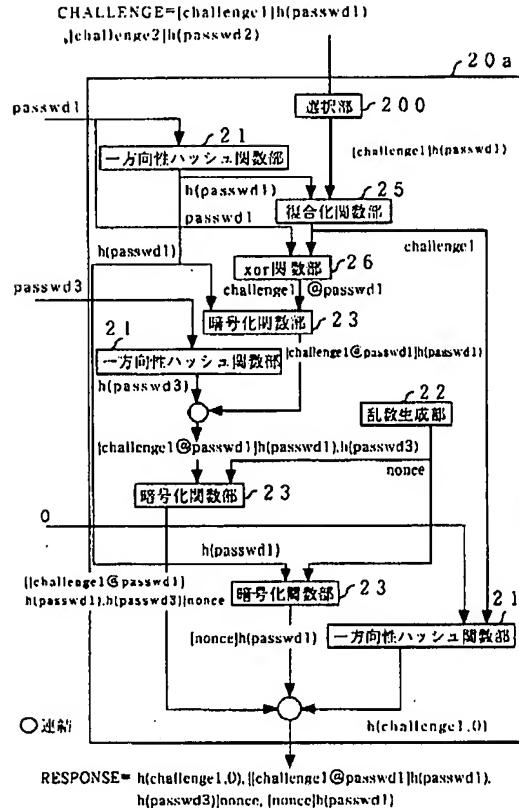


【図13】



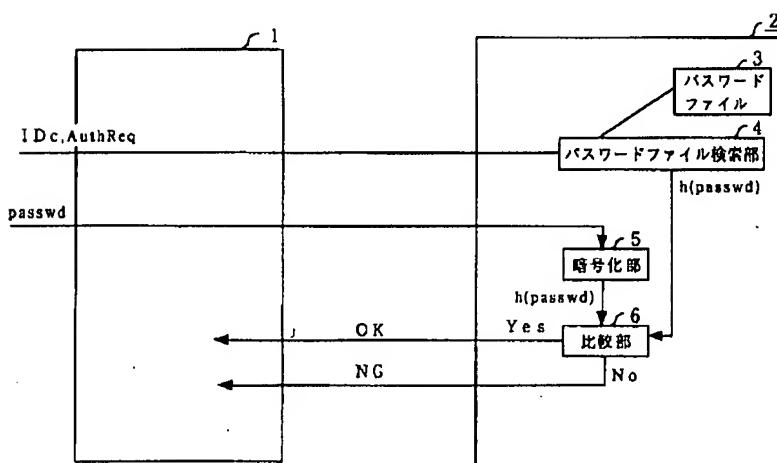
○ 連続

【図15】

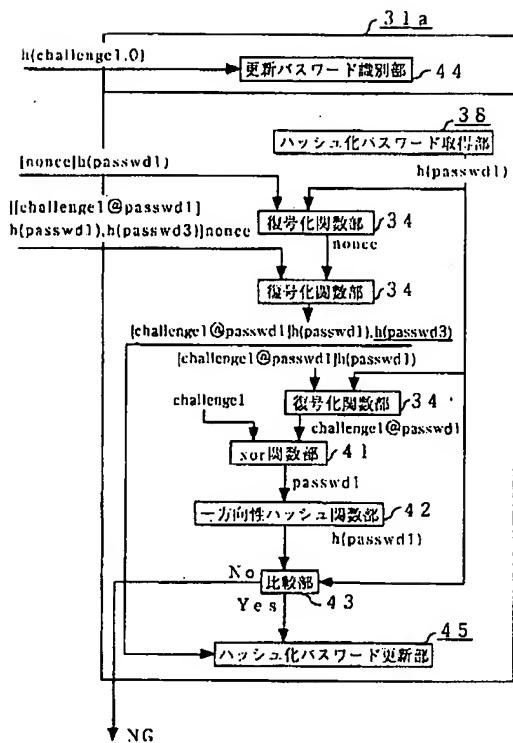


○ 連続

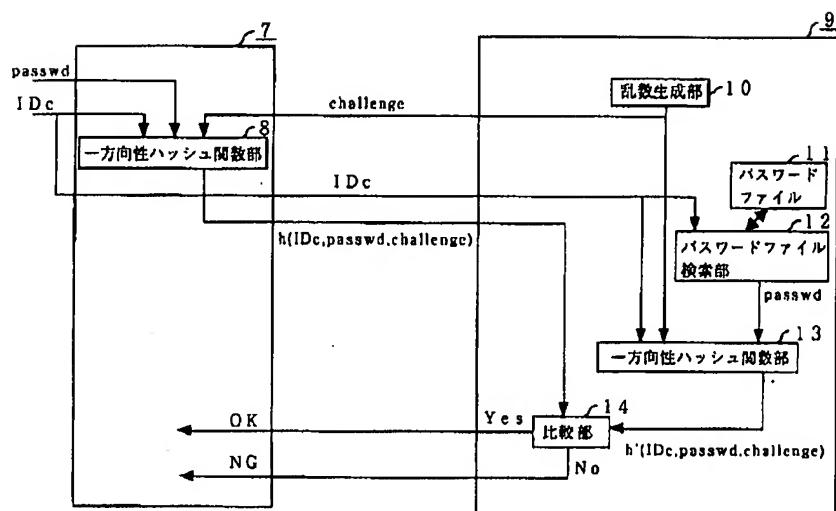
【図17】



【図16】



【図18】



【図19】

